GRUPA SANTANDER

WIĄŻĄCE REGUŁY KORPORACYJNE – POLITYKA ADMINISTRATORA DANYCH

SPIS TREŚCI STRONA

WPROWADZENIE

Niniejsza Polityka Wiążących Reguł Korporacyjnych - Administratora Danych wraz z jej załącznikami (łącznie „**Polityka**") określa zasady ochrony danych osobowych oraz zarządzania nimi przyjęte przez Banco Santander, S.A. („**Banco Santander**"), stosowane przez członków Grupy Santander, zgodnie z definicją poniżej, którzy przystąpili do niniejszej Polityki, w związku z międzynarodowym przekazywaniem danych osobowych pomiędzy Członkami Grupy, zgodnie z definicją poniżej.

Banco Santander jest spółką dominującą oraz centralą jednej z największych grup finansowych w Hiszpanii, obejmującej zarówno hiszpańskie, jak i zagraniczne spółki zależne („**Grupa Santander**"), świadczącej usługi finansowe na całym świecie, przede wszystkim w następujących obszarach: (i) **Bankowość detaliczna i komercyjna** - obejmuje całość działalności Santander w obszarze bankowości detalicznej i komercyjnej; (ii) **Bankowość korporacyjna i inwestycyjna** - zapewnia klientom korporacyjnym i instytucjonalnym dostosowane do ich potrzeb usługi oraz specjalistyczne produkty bankowości hurtowej o wartości dodanej za pośrednictwem jednostek Markets, Investment Banking (Global Debt Finance i Corporate Finance) oraz Global Transactional Banking; (iii) **Zarządzanie majątkiem i ubezpieczenia** - obejmuje bankowość prywatną, zarządzanie aktywami oraz działalność ubezpieczeniową za pośrednictwem Santander Private Banking, Santander Asset Management i Santander Insurance; (iv) **Cyfrowy Bank Konsumencki** - łączy cyfrową platformę Openbank oraz Santander Consumer Finance, tworząc jednolity model działalności na wszystkich rynkach dla klientów detalicznych oraz w zakresie finansowania pojazdów; oraz (v) **PagoNxt i Karty** - obejmuje PagoNxt, skupiający całą działalność Grupy Santander w zakresie usług płatniczych, oraz Global Cards, obszar działalności kartowej i platformę kartową Santander, oferujące cyfrowe rozwiązania płatnicze oraz globalne rozwiązania technologiczne dla banków Grupy Santander i nowych klientów. Ponadto Grupa Santander obejmuje również **Centrum Korporacyjne oraz inne funkcje wspólne świadczące usługi na rzecz całej Grupy**, odpowiedzialne za zapewnianie wsparcia wszystkim Członkom Grupy w realizacji działań na poziomie Grupy, które nie są bezpośrednio związane z ich podstawową działalnością (*np.* zarządzanie personelem, zapewnianie zgodności z przepisami prawa, audyt czy zarządzanie ryzykiem).

Oprócz pozostałych definicji zawartych w niniejszej Polityce obowiązują następujące definicje:

„**właściwe lokalne prawo ochrony danych**" oznacza krajowe lub lokalne przepisy o ochronie danych (w tym, w zależności od okoliczności, europejskie prawo ochrony danych) mające zastosowanie do Członków Grupy, o ile nie naruszają istoty podstawowych praw i wolności oraz nie wykraczają poza to, co jest konieczne i proporcjonalne w społeczeństwie demokratycznym, zgodnie z wymogami Zasady 13 niniejszej Polityki;

„**właściwy organ nadzorczy**" oznacza organ nadzorczy państwa EOG właściwy dla Podmiotu Eksportującego;

„**administrator danych**" oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

„**Europa**" lub „**EOG**" oznacza państwa należące do Europejskiego Obszaru Gospodarczego;

„**Europejskie Prawo Ochrony Danych**" oznacza RODO oraz wszelkie przepisy o ochronie danych obowiązujące w państwie członkowskim EOG, w tym przepisy krajowe uzupełniające RODO, w szczególności akty wykonawcze, wraz z ich późniejszymi zmianami;

„**Podmiot Eksportujący**" oznacza Członka Grupy mającego siedzibę w Europie lub w inny sposób podlegającego europejskiemu prawu ochrony danych, który przekazuje lub w inny sposób udostępnia dane osobowe Podmiotowi Importującemu zgodnie z niniejszą Polityką;

„**RODO**" oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (ogólne rozporządzenie o ochronie danych);

„**Członek Grupy**" oznacza członka Grupy Santander, który przystąpił do niniejszej Polityki;

„**Podmiot Importujący**" oznacza Członka Grupy mającego siedzibę poza Europą, który otrzymuje dane osobowe od Podmiotu Eksportującego i przetwarza je poza EOG;

„**Odpowiedzialny Członek BCR**" oznacza Banco Santander (tj. Banco Santander, S.A., zgodnie z definicją powyżej);

„**dane osobowe**" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. 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 tej osoby;

„**przetwarzanie**" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zbiorach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

„**podmiot przetwarzający**" oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

„**profilowanie**" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych polegającą na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych dotyczących osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, stanu zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

„**szczególne kategorie danych osobowych**" lub „**dane wrażliwe**" oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia lub dane dotyczące życia seksualnego bądź orientacji seksualnej osoby fizycznej; oraz

„**organ nadzorczy**" oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie EOG, odpowiedzialny za monitorowanie stosowania europejskiego prawa ochrony danych w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych oraz ułatwiania swobodnego przepływu danych osobowych w EOG.

Niniejsza Polityka ma zastosowanie do wszystkich danych osobowych podlegających europejskiemu prawu ochrony danych, które są następnie przekazywane przez Podmioty Eksportujące do Podmiotów Importujących, a także dalej przekazywane przez Podmioty Importujące innym Podmiotom Importującym lub podmiotom trzecim poza EOG (zgodnie z wymogami określonymi w Zasadzie 6 poniżej). W związku z tym wszelkie obowiązki i wymogi nałożone na Członków Grupy na mocy niniejszej Polityki mają zastosowanie w zakresie, w jakim odnoszą się do danych osobowych objętych zakresem jej stosowania.

Niniejsza Polityka ma zastosowanie do wszystkich takich danych osobowych przetwarzanych przez Członków Grupy, zgodnie z opisem zawartym w sekcjach *„Jakie dane osobowe obejmuje niniejsza Polityka*?" oraz *„W jakich celach dane osobowe są przekazywane na podstawie niniejszej Polityki?*".

Członkowie Grupy oraz ich pracownicy są zobowiązani do pełnego przestrzegania postanowień niniejszej Polityki przy przetwarzaniu danych osobowych objętych jej zakresem.

Niniejsza Polityka stanowi uzupełnienie i nie zastępuje ani nie uchyla szczególnych wymogów lub zasad dotyczących poufności bądź obowiązku zachowania tajemnicy, które mogą mieć zastosowanie do określonego obszaru działalności lub funkcji w ramach Grupy Santander albo wynikać z obowiązujących przepisów prawa (o ile przepisy te są zgodne z wymogami określonymi w Zasadzie 13 niniejszej Polityki).

Niniejsza Polityka wraz z listą aktualnych Członków Grupy oraz ich danymi kontaktowymi zawartą w Załączniku 5 jest publikowana na publicznie dostępnej stronie internetowej spółki tutaj.

Zastosowanie do międzynarodowego przekazywania danych osobowych przez Członków Grupy niepodlegających europejskiemu prawu ochrony danych

Jeżeli Członek Grupy niepodlegający europejskiemu prawu ochrony danych podlega również ograniczeniom dotyczącym międzynarodowego przekazywania danych osobowych wynikającym z właściwego lokalnego prawa ochrony danych, a właściwe organy tych państw uznają niniejszą Politykę (w całości lub w części, zgodnie z wymogami właściwego lokalnego prawa ochrony danych) za mechanizm uznawany za podstawę zgodnego z prawem międzynarodowego przekazywania danych osobowych, niniejsza Polityka może mieć również zastosowanie do danych osobowych przekazywanych z tych państw do Podmiotów Importujących. Dla uniknięcia wątpliwości pozostaje to bez wpływu na stosowanie wobec Członka Grupy spoza Europy właściwego lokalnego prawa ochrony danych.

W takich przypadkach powyższe definicje należy rozumieć w ten sposób, że Członek Grupy przekazujący dane osobowe niepodlegające europejskiemu prawu ochrony danych jest traktowany jako Podmiot Eksportujący. W związku z tym niniejszą Politykę należy interpretować i stosować *mutatis mutandis* (*np.* europejskie prawo ochrony danych należy odpowiednio rozumieć jako właściwe lokalne prawo ochrony danych, właściwy organ nadzorczy jako właściwy organ lokalny w danej jurysdykcji, a państwo członkowskie jako dane państwo).

W tym kontekście Członek Grupy przekazujący dane osobowe, które nie podlegają europejskiemu prawu ochrony danych, będzie pełnił rolę Odpowiedzialnego Członka BCR w odniesieniu do takiego międzynarodowego przekazywania danych.

CZĘŚĆ I: TŁO I DZIAŁANIA

CZYM JEST EUROPEJSKIE PRAWO OCHRONY DANYCH?

Europejskie prawo ochrony danych przyznaje osobom fizycznym prawo do sprawowania kontroli nad sposobem przetwarzania ich danych osobowych. Zgodnie z europejskim prawem ochrony danych, gdy organizacja przetwarza dane osobowe na własne potrzeby, uznaje się ją za administratora danych, a tym samym ponosi ona główną odpowiedzialność za spełnienie obowiązujących wymogów prawnych. Na przykład jako pracodawca jesteśmy administratorem danych osobowych naszych pracowników.

Natomiast gdy organizacja przetwarza dane osobowe w imieniu innego podmiotu (na przykład w celu świadczenia usług), uznaje się ją za podmiot przetwarzający.

JAK EUROPEJSKIE PRAWO OCHRONY DANYCH WPŁYWA NA PRZEKAZYWANIE DANYCH OSOBOWYCH MIĘDZY CZŁONKAMI GRUPY?

Europejskie prawo ochrony danych nie dopuszcza przekazywania danych osobowych do państw, terytoriów lub organizacji międzynarodowych poza Europą, które nie zapewniają odpowiedniego poziomu ochrony praw osób, których dane dotyczą. Ponieważ niektóre państwa, w których działają Członkowie Grupy, nie zostały uznane przez Komisję Europejską za zapewniające odpowiedni stopień ochrony, konieczne jest wdrożenie odpowiednich zabezpieczeń w celu spełnienia wymogów europejskiego prawa ochrony danych.

CO W TEJ SPRAWIE ROBIĄ CZŁONKOWIE GRUPY?

Członkowie Grupy są zobowiązani do podjęcia odpowiednich działań w celu zapewnienia, że przetwarzanie danych osobowych w ramach ich międzynarodowego przekazywania odbywa się w sposób bezpieczny i zgodny z prawem. Celem niniejszej Polityki jest zatem ustanowienie ram zapewniających zgodność z wymogami określonymi w europejskim prawie ochrony danych, a w konsekwencji zapewnienie odpowiedniego poziomu ochrony wszystkich danych osobowych przekazywanych przez Podmioty Eksportujące do Podmiotów Importujących.

Niniejsza Polityka ma charakter wiążący i ma zastosowanie do wszystkich Członków Grupy oraz ich pracowników w zakresie przetwarzania przez Członków Grupy danych osobowych, zarówno w sposób zautomatyzowany, jak i niezautomatyzowany. Na mocy niniejszej Polityki Członkowie Grupy są zobowiązani do przestrzegania Zasad określonych w Części II niniejszej Polityki (w odpowiednim zakresie), a także polityk i procedur określonych w Załącznikach zamieszczonych w Części III niniejszej Polityki. Jeżeli Podmiot Importujący podlega właściwemu lokalnemu prawu ochrony danych, które jest uznawane, na gruncie właściwego lokalnego prawa ochrony danych Podmiotu Eksportującego, za zapewniające odpowiedni stopień ochrony oraz gwarantuje poziom ochrony równoważny poziomowi określonemu w niniejszej Polityce, lokalne procesy i procedury, które w istotnym stopniu spełniają wymogi niniejszej Polityki, będą uznawane za zgodne z jej postanowieniami, nawet jeśli przewidują odstępstwa lub różnice proceduralne (*np.* wykonywanie określonych procedur przez lokalne zespoły), pod warunkiem że pozostają zgodne z niniejszą Polityką. Międzynarodowe przekazywanie danych osobowych objęte niniejszą Polityką obejmuje przekazywanie danych osobowych z Podmiotów Grupy objętych terytorialnym zakresem stosowania RODO zgodnie z art. 3 RODO do Podmiotów Grupy poza EOG, a także dalsze przekazywanie danych do innych Podmiotów Grupy lub podmiotów trzecich spoza Grupy poza EOG (zgodnie z wymogami określonymi w Zasadzie 6 poniżej).

JAKIE ZASADY MAJĄ ZASTOSOWANIE DO CZŁONKÓW GRUPY NIEPODLEGAJĄCYCH EUROPEJSKIEMU PRAWU OCHRONY DANYCH, KTÓRZY PRZEKAZUJĄ DANE OSOBOWE?

Jak wyjaśniono we Wprowadzeniu, w celu ustanowienia jednolitych globalnych ram ochrony danych w Grupie Santander, jeżeli Członek Grupy niepodlegający europejskiemu prawu ochrony danych podlega również ograniczeniom dotyczącym międzynarodowego przekazywania danych osobowych wynikającym z właściwego lokalnego prawa ochrony danych, a właściwe organy tych państw uznają niniejszą Politykę (w całości lub w części, zgodnie z wymogami właściwego lokalnego prawa ochrony danych) za mechanizm uznawany za podstawę zgodnego z prawem międzynarodowego przekazywania danych osobowych, niniejsza Polityka może mieć również zastosowanie do danych osobowych przekazywanych z tych państw do Podmiotów Importujących. Dla uniknięcia wątpliwości pozostaje to bez wpływu na stosowanie wobec Członka Grupy spoza Europy właściwego lokalnego prawa ochrony danych.

JAKIE DANE OSOBOWE OBEJMUJE NINIEJSZA POLITYKA?

Zakres danych osobowych przetwarzanych na podstawie niniejszej Polityki obejmuje:

- W odniesieniu do danych osobowych **obecnych i byłych pracowników oraz innych członków personelu (takich jak stażyści, pracownicy oddelegowani lub niezależni współpracownicy)**:

  (a) Dane osobowe i dane kontaktowe (*np.* imię, drugie imię, nazwisko, tytuł, pseudonim, podpis, płeć, data urodzenia, obywatelstwo, krajowe numery identyfikacyjne lub dokumenty tożsamości, adres e-mail, adres zamieszkania, numery telefonów, fotografia, zezwolenia na pracę itp.); **(b) Dane dotyczące zatrudnienia, w tym przebiegu zatrudnienia, warunków zatrudnienia oraz dane kontaktowe** (*np.* służbowy adres e-mail i numer telefonu, numer identyfikacyjny pracownika, przydzielona nazwa użytkownika lub klucz adresowy (tj. wykorzystywany do uzyskania dostępu do terminala stacji roboczej), historia zatrudnienia, aktualne stanowisko, rola, zakres obowiązków, spółka, centrum operacyjne, jednostka organizacyjna, numer identyfikacyjny działu, numer identyfikacyjny oddziału, kraj prowadzenia działalności, identyfikator oraz imię i nazwisko przełożonego(-ych), identyfikator oraz imię i nazwisko podwładnego(-ych), status i rodzaj zatrudnienia, informacja, czy dana osoba jest pracownikiem zewnętrznym, data zatrudnienia, data objęcia stanowiska, data zakończenia zatrudnienia (jeżeli dotyczy), informacje dotyczące umowy o pracę, programy emerytalne, elastyczne formy organizacji pracy, wnioski o przeniesienie, przydzielone wyposażenie służbowe, informacje dotyczące przestrzegania polityk wewnętrznych oraz obowiązujących przepisów prawa, oceny okresowe (w tym informacje zwrotne od przełożonych, interesariuszy i innych osób współpracujących z pracownikiem), awanse oraz informacje dotyczące postępowań dyscyplinarnych itp.); **(c) Dane dotyczące rozwoju zawodowego, rekrutacji, wykształcenia i szkoleń** (*np.* informacje zawarte w listach motywacyjnych i życiorysach (CV), informacje dotyczące indywidualnego planu rozwoju oraz ocen pracowniczych, informacje o odbytych szkoleniach, adres osobistej strony internetowej lub profil w serwisie LinkedIn udostępniony przez pracownika, historia wcześniejszego zatrudnienia i referencje, wykształcenie, kwalifikacje zawodowe, znajomość języków oraz inne istotne umiejętności itp.); **(d) Dane finansowe, w tym dane dotyczące rozliczeń płacowych i wynagrodzeń** (*np.* dane rachunku bankowego, wynagrodzenie, programy świadczeń, premie, waluta, zmienne składniki wynagrodzenia, informacje dotyczące opcji na akcje, przyznanych akcji i innych świadczeń, częstotliwość wypłat, data obowiązywania aktualnego wynagrodzenia, przeglądy wynagrodzeń, identyfikator podatkowy i kod podatkowy itp.); **(e) Dane dotyczące bezpieczeństwa oraz systemów IT** (*np.* identyfikator użytkownika, dane logowania, klucze dostępu do narzędzi, poświadczenia i profile bezpieczeństwa, wiadomości e-mail wysyłane z firmowych kont poczty elektronicznej i odbierane na tych kontach, w zakresie dozwolonym przez prawo, informacje pozyskiwane w związku z korzystaniem z systemów IT, w tym informacje o dostępie i uwierzytelnianiu, historia przeglądania stron internetowych, wybierane numery telefonów, dokumenty i pliki przechowywane w systemach lub sieciach spółki (w tym na dyskach komputerów służbowych), dzienniki systemowe, adresy IP, udane i nieudane próby logowania,

informacje gromadzone za pomocą plików cookie lub innych podobnych technologii śledzących itp.; **(f) Dane dotyczące czasu pracy** (*np.* urlopy, dni wolne, inne nieobecności oraz dokumenty potwierdzające ich przyczyny (jeżeli dotyczy), daty powrotu do pracy po zakończeniu nieobecności, ewidencja czasu pracy (w przypadkach wymaganych lub dopuszczonych przez prawo), godziny nadliczbowe, harmonogramy czasu pracy itp.); oraz **(g) Wszelkie inne informacje dobrowolnie przekazane przez osoby, których dane dotyczą** (*np.* za pośrednictwem ankiet dotyczących zaangażowania pracowników lub innych ankiet itp.).

Ponadto **szczególne kategorie danych osobowych (w szczególności, choć nie wyłącznie, dane dotyczące zdrowia oraz przynależności do związków zawodowych)** mogą być przetwarzane przez Członków Grupy, jeżeli jest to konieczne oraz wymagane lub dozwolone na mocy obowiązujących przepisów prawa, do celów opisanych w kolejnej sekcji.

- W odniesieniu do **danych osobowych członków** rodzin pracowników:

  (a) Dane osobowe i dane kontaktowe (*np.* imię, nazwisko, płeć, krajowe numery identyfikacyjne lub dokumenty tożsamości, dane kontaktowe, takie jak numer telefonu osoby do kontaktu w nagłych przypadkach itp.); oraz **(b) Inne informacje dotyczące pracowników lub członków ich rodzin, jeżeli jest to wymagane lub dozwolone przez prawo** (*np.* skład rodziny i sytuacja rodzinna, relacja z pracownikiem, imiona oraz inne istotne informacje dotyczące dzieci i innych osób pozostających na utrzymaniu, stan cywilny, informacje dotyczące przestrzegania polityk wewnętrznych oraz obowiązujących przepisów prawa itp.).

- W odniesieniu do danych osobowych **obecnych i byłych kandydatów do pracy**:

  (a) Dane osobowe i dane kontaktowe (*np.* imię, nazwisko, kraj, stan/prowincja i miasto zamieszkania, adres e-mail, adres zamieszkania, numery telefonów, obywatelstwo itp.); **(b) Dane dotyczące rekrutacji, wykształcenia i szkoleń** (*np.* informacje zawarte w listach motywacyjnych i życiorysach (CV), na osobistej stronie internetowej lub w profilu w serwisie LinkedIn udostępnionym przez kandydata, informacje dotyczące dotychczasowego doświadczenia zawodowego i referencji, wykształcenia, kwalifikacji zawodowych, znajomości języków oraz innych istotnych umiejętności, informacje dotyczące ocen, indywidualnego planu rozwoju oraz gotowości do relokacji, dane osobowe uzyskane w związku z udziałem kandydata w procesie rekrutacji, w tym podczas rozmów kwalifikacyjnych oraz z korespondencji e-mail prowadzonej w związku z procesem rekrutacji itp.); oraz **(c) Dane dźwiękowe i wizualne** (*np.* głos i wizerunek utrwalone na fotografiach oraz nagraniach audio lub wideo wykonanych podczas rozmów kwalifikacyjnych prowadzonych telefonicznie lub za pośrednictwem wideokonferencji itp.).

- W odniesieniu do danych osobowych **potencjalnych klientów, klientów i kontrahentów** (w tym, w stosownych przypadkach, ich pracowników, przedstawicieli, agentów, upoważnionych użytkowników oraz użytkowników strony internetowej):

  (a) Dane osobowe i dane kontaktowe *(np.* imię, drugie imię, nazwisko, numer telefonu, adres e-mail, adres pocztowy, kraj zamieszkania, region, obywatelstwo lub narodowość, krajowe numery identyfikacyjne lub dokumenty tożsamości, płeć, język, data urodzenia, kraj urodzenia, stan cywilny, dane dotyczące sytuacji rodzinnej lub społecznej (*np.* liczba osób pozostających na utrzymaniu), informacja, czy dana osoba jest małoletnia lub wymaga przedstawiciela ustawowego, dane demograficzne i społeczno-ekonomiczne itp.); **(b) Dane zawodowe** *(np.* zawód, stanowisko, przebieg zatrudnienia i wykształcenia, dane dotyczące spółki, służbowe dane kontaktowe, wykonywany zawód, kategoria zawodowa, nazwa stanowiska itp.); **(c) Dane (przed)umowne** (*np.* kod kategorii, zdolność do czynności prawnych, dane dotyczące pełnomocnictw, numer rejestracyjny i wewnętrzny identyfikator klienta, stopień powiązania, relacja biznesowa z Santander, produkty lub usługi objęte umową lub

zamówione, ocena ryzyka (scoring), informacje z biur informacji kredytowej, zamówienia zakupu, dane statystyczne, faktury, informacje dotyczące majątku i aktywów, dotacje, informacje dotyczące rachunków i transakcji, w zakresie dozwolonym przez obowiązujące przepisy prawa, umowy i inne porozumienia zawierające dane osobowe tych osób oraz informacje dotyczące wykonywania tych umów itp.); **(d) Informacje finansowe, podatkowe i dotyczące płatności** (*np.* dane rachunku bankowego, dane beneficjenta, aktualne i historyczne salda produktów i usług oraz historia płatności, dane kart płatniczych, polecenia wypłaty wynagrodzenia, informacje o dochodach i ich rodzaju, dostępne środki, transakcje pieniężne, kwoty płatności, dane dotyczące przekazów pieniężnych, informacje dotyczące wypłacalności, numer identyfikacji podatkowej, kraj rezydencji podatkowej, roczne rozliczenie podatkowe itp.); **(e) Dane dotyczące zgodności z przepisami** (*np.* identyfikacja osoby zajmującej eksponowane stanowisko polityczne (PEP) lub osoby z nią powiązanej, powiązania wynikające z przepisów MiFID lub podobnych regulacji (*np.* współpracownicy, więzi rodzinne itp.), rodzaj relacji (*np.* małżonek, krewny, akcjonariusz, przedstawiciel ustawowy itp.), data rozpoczęcia relacji oraz, jeżeli dotyczy, data jej zakończenia, informacje związane z obowiązkami w zakresie przeciwdziałania praniu pieniędzy (AML) oraz przeciwdziałania nadużyciom, w tym profile, informacje z baz danych dotyczących wypłacalności i ryzyka oraz oceny punktowe (scoring) itp.); **(f) Dane dźwiękowe i wizualne** (*np.* głos i wizerunek utrwalone na fotografiach oraz nagraniach audio lub wideo wykonanych podczas spotkań prowadzonych telefonicznie lub za pośrednictwem wideokonferencji albo na potrzeby zapewnienia bezpieczeństwa itp.); (g) **Dane dotyczące systemów IT** (*np.* adres IP, identyfikator użytkownika, hasła, dzienniki systemowe (w tym informacje o profilu) dotyczące stron internetowych lub portali Grupy Santander, klucze dostępu do narzędzi, poświadczenia i profile bezpieczeństwa, dane uwierzytelniające, historia przeglądania stron internetowych, identyfikator urządzenia, identyfikator reklamowy, informacje dotyczące mediów społecznościowych itp.); oraz (h) **Inne informacje dotyczące relacji z Grupą Santander** (*np.* dane dotyczące reklamacji i skarg, dotychczasowa komunikacja, preferencje komunikacyjne, wnioski itp.).

Ponadto **szczególne kategorie danych osobowych oraz dane osobowe dotyczące wyroków skazujących i czynów zabronionych** (w kontekście ryzyk oraz sankcji międzynarodowych) mogą być przetwarzane przez Członków Grupy, jeżeli jest to konieczne oraz wymagane lub dozwolone na mocy obowiązujących przepisów prawa, do celów opisanych w kolejnej sekcji.

- W odniesieniu do danych osobowych **potencjalnych i obecnych dostawców oraz usługodawców** (w tym, w stosownych przypadkach, ich pracowników, przedstawicieli i agentów):

  (a) Dane osobowe, zawodowe i kontaktowe (*np.* imię, nazwisko, numer telefonu, adres e-mail, adres pocztowy, krajowe numery identyfikacyjne lub dokumenty tożsamości, stanowisko lub funkcja, dane dotyczące spółki, służbowe dane kontaktowe itp.); **(b) Dane umowne** (*np.* dane dotyczące pełnomocnictw, zamówienia zakupu, faktury, umowy i inne porozumienia mogące zawierać dane osobowe tych osób itp.); **(c) Dane finansowe i dotyczące płatności** *(np.* dane rachunku bankowego, dane kart płatniczych, informacje dotyczące wypłacalności itp.); **(d) Dane dźwiękowe i wizualne** *(np.* głos i wizerunek utrwalone na fotografiach oraz nagraniach audio lub wideo wykonanych podczas spotkań prowadzonych telefonicznie lub za pośrednictwem wideokonferencji albo na potrzeby zapewnienia bezpieczeństwa, w tym informacje gromadzone przez systemy kontroli dostępu i kamery monitoringu itp.); **(e) Dane dotyczące systemów IT** *(np.* adres IP, identyfikator użytkownika, hasła, dzienniki systemowe (w tym informacje o profilu) dotyczące stron internetowych lub portali Grupy Santander itp.); oraz **(f) Inne informacje dotyczące relacji zawodowej z Grupą Santander** *(np.* dane dotyczące reklamacji i skarg, dotychczasowa komunikacja itp.).

- W odniesieniu do danych osobowych **akcjonariuszy**:

  (a) Dane osobowe, zawodowe i kontaktowe (*np.* imię, nazwisko, płeć, data urodzenia, numer telefonu, adres e-mail, adres pocztowy, krajowe numery identyfikacyjne lub dokumenty tożsamości, stanowisko

lub funkcja, dane dotyczące spółki, służbowe dane kontaktowe, numer akcjonariusza, obywatelstwo lub narodowość, kraj urodzenia i zamieszkania itp.); **(b) Dane finansowe i dotyczące płatności** (*np.* dane rachunku bankowego, dane kart płatniczych, dane dotyczące płatności, liczba posiadanych akcji, dokumenty potwierdzające prawo własności oraz prawo do dywidendy, transakcje pieniężne, transakcje na akcjach, stan posiadania oraz udziały w innych spółkach, informacje o zawartych umowach dotyczących produktów finansowych itp.); oraz **(c) Dane dotyczące systemów IT** *(np.* adres IP, identyfikator użytkownika, hasła, dzienniki systemowe (w tym informacje o profilu) dotyczące stron internetowych lub portali Grupy Santander itp.).

- W odniesieniu do danych osobowych **użytkowników stron internetowych, użytkowników końcowych oraz użytkowników instytucjonalnych (w tym użytkowników platform, stron internetowych i aplikacji związanych z uczelniami, zatrudnieniem oraz przedsiębiorczością):**

  (a) Dane osobowe i dane kontaktowe (*np.* imię, nazwisko, data urodzenia, płeć, adres e-mail, adres pocztowy, numery telefonów, kraj zamieszkania, obywatelstwo, krajowe numery identyfikacyjne itp.); **(b) Dane zawodowe i edukacyjne** (*np.* stanowisko lub funkcja, dane dotyczące spółki, służbowe dane kontaktowe, przebieg zatrudnienia, życiorys (CV), informacje dotyczące wykształcenia lub kwalifikacji, dane demograficzne i społeczno-ekonomiczne, powiązania z projektami przedsiębiorczymi lub spółkami itp.); **(c) Dane dotyczące systemów IT** (*np.* adres IP, identyfikator użytkownika, hasła, dzienniki aktywności użytkownika (w tym informacje o profilu) dotyczące korzystania ze stron internetowych lub portali, rejestry połączeń itp.); **(d) Dane dotyczące korzystania ze stron internetowych i urządzeń** (*np.* informacje gromadzone automatycznie za pomocą plików cookie lub innych podobnych technologii dotyczące korzystania ze stron internetowych lub urządzeń, informacje o profilu użytkownika, historii przeglądania oraz sposobie korzystania z usług itp.); oraz **(e) Inne informacje dotyczące relacji z Grupą Santander** *(np.* zapytania, zainteresowania, dotychczasowa komunikacja itp.).

W JAKICH CELACH DANE OSOBOWE SĄ PRZEKAZYWANE NA PODSTAWIE NINIEJSZEJ POLITYKI?

Dane osobowe są przekazywane pomiędzy Członkami Grupy na całym świecie (głównie do Argentyny, Bahamów, Brazylii, Kolumbii, państw europejskich, Meksyku, Peru, Szwajcarii, Wielkiej Brytanii, Stanów Zjednoczonych Ameryki, Urugwaju itd.) na podstawie niniejszej Polityki wyłącznie w następujących celach i tylko w zakresie dozwolonym przez obowiązujące przepisy prawa:

- Przekazywanie **danych osobowych obecnych i byłych pracowników oraz innych członków personelu (takich jak stażyści, pracownicy oddelegowani lub niezależni współpracownicy)** odbywa się w celu: **(a) zarządzania personelem** (*np.* zarządzania szkoleniami, planowania i monitorowania działań kadrowych, zarządzania wynikami pracy, wynagrodzeniami i świadczeniami, awansami, planowania sukcesji i rozwoju kariery, zarządzania mobilnością wewnętrzną, przeniesieniami i oddelegowaniami, prowadzenia rejestrów pracowników, organizowania podróży służbowych, zarządzania wydatkami służbowymi i zwrotem kosztów, zapewnienia sprawnej komunikacji biznesowej, prowadzenia negocjacji, zawierania transakcji i organizowania konferencji, weryfikacji wykonywania przez pracowników obowiązków wynikających ze stosunku pracy, zarządzania urlopami i nieobecnościami, przeprowadzania ocen okresowych, prowadzenia i dokumentowania postępowań dyscyplinarnych oraz rozwiązywania stosunku pracy, weryfikacji decyzji kadrowych, podejmowania decyzji dotyczących zdolności do pracy oraz dostosowania stanowiska pracy, monitorowania zgodności z politykami i procedurami wewnętrznymi oraz prowadzenia innych czynności monitorujących wymaganych przez obowiązujące przepisy prawa (*np.* w ramach wewnętrznych systemów zgłaszania nieprawidłowości), w tym zapewnienia zgodności z Kodeksem postępowania na rynkach papierów wartościowych lub podobnymi politykami oraz związanymi z nimi obowiązkami, w tym zatwierdzania i monitorowania transakcji na rachunek własny, prowadzenia analiz i planowania zasobów kadrowych oraz przeprowadzania weryfikacji przeszłości zgodnie z

obowiązującymi przepisami prawa); **(b) przeprowadzania zagregowanych analiz i segmentacji** dotyczących aktywności pracowników w celu lepszego poznania grupy pracowników oraz wspierania podejmowania decyzji dotyczących między innymi pozyskiwania talentów, planowania kariery i planowania sukcesji; **(c) wspierania zarządzania usługami świadczonymi przez Grupę Santander oraz jej działalnością operacyjną** (*np.* zarządzania systemami i infrastrukturą IT oraz komunikacyjną i zapewniania ich bezpieczeństwa, zarządzania majątkiem spółki, zasobami ludzkimi, wyposażeniem biurowym i innym mieniem oraz ich przydzielania, planowania operacyjnego i strategicznego, zarządzania projektami, zapewniania ciągłości działania, tworzenia ścieżek audytowych i innych narzędzi sprawozdawczych, prowadzenia dokumentacji działalności biznesowej, budżetowania, zarządzania finansami i sprawozdawczości, komunikacji, zarządzania fuzjami, przejęciami, reorganizacjami oraz zbywaniem działalności); oraz **(d) wywiązywania się z obowiązków prawnych i innych wymogów** (*np.* obowiązków w zakresie ochrony danych osobowych, podatków i ubezpieczeń społecznych, prawa pracy, zarządzania ryzykiem, przeciwdziałania nadużyciom, zgłaszania nieprawidłowości, prowadzenia wymaganej dokumentacji i sprawozdawczości, dochodzenia praw i roszczeń, obrony w postępowaniach sądowych, zapewnienia zgodności z kontrolami prowadzonymi przez organy administracji publicznej oraz realizacji innych żądań właściwych organów, udzielania odpowiedzi na wezwania i inne czynności procesowe, wykonywania obowiązków wynikających z prawa pracy i ubezpieczeń społecznych, przeprowadzania audytów oraz rozpatrywania skarg i roszczeń wewnętrznych).

W odniesieniu do **szczególnych kategorii danych osobowych pracowników (w tym, o ile jest to dopuszczalne, danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych)** dane te mogą być przetwarzane przez Członków Grupy, jeżeli jest to niezbędne do realizacji celów określonych w niniejszej Polityce (*np.* wywiązywania się z obowiązków prawnych, zarządzania zasobami ludzkimi, obsługi kanału zgłaszania nieprawidłowości, zarządzania wynagrodzeniami i świadczeniami, zarządzania mobilnością wewnętrzną, przeniesieniami i oddelegowaniami, przeprowadzania zagregowanych analiz i segmentacji, sporządzania statystyk i prowadzenia analiz itp.), wyłącznie w zakresie niezbędnym do wykonywania obowiązków oraz korzystania ze szczególnych praw przysługujących Członkom Grupy lub osobie, której dane dotyczą, w dziedzinie prawa pracy oraz zabezpieczenia społecznego i ochrony socjalnej (art. 9 ust. 2 lit. b RODO), a także do celów medycyny zapobiegawczej lub medycyny pracy, oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub społecznej, leczenia oraz zarządzania systemami i usługami opieki zdrowotnej lub społecznej (art. 9 ust. 2 lit. h RODO).

- Przekazywanie danych osobowych **członków rodzin pracowników** odbywa się w celu zarządzania relokacją pracowników za granicę, przeprowadzania zagregowanych analiz i segmentacji, sporządzania statystyk i prowadzenia analiz, monitorowania zgodności z Kodeksem postępowania na rynkach papierów wartościowych lub podobnymi politykami oraz związanymi z nimi obowiązkami, w tym zatwierdzania i monitorowania transakcji na rachunek własny, a także zarządzania świadczeniami pracowniczymi (*np.* w zakresie ubezpieczeń).

- Przekazywanie danych osobowych **obecnych i byłych kandydatów** odbywa się w celu prowadzenia krajowych i międzynarodowych procesów rekrutacyjnych (*np.* oceny kandydatur i podejmowania decyzji o zatrudnieniu, komunikacji z kandydatami w związku z procesem rekrutacji lub złożonymi zgłoszeniami itp.).

- Przekazywanie danych osobowych **potencjalnych klientów, klientów i kontrahentów** (w tym danych ich pracowników, przedstawicieli i/lub agentów, upoważnionych użytkowników oraz użytkowników stron internetowych) odbywa się w następujących celach: **(a) zarządzania relacjami umownymi z klientami oraz świadczenia usług** *(np.* wydawania kart płatniczych, w tym upoważnionym użytkownikom kart korporacyjnych, oferowania usług płatniczych i usług bankowości internetowej oraz zarządzania nimi, prowadzenia rejestrów w celu zapewnienia spójności informacji pomiędzy

różnymi jurysdykcjami, zawierania umów oraz podejmowania działań zmierzających do ich zawarcia, w tym prowadzenia procesów KYC, prowadzenia działalności gospodarczej i komunikacji biznesowej, przenoszenia rachunków, nawiązywania, odnawiania, utrzymywania i rozwiązywania relacji biznesowych, zapewniania dostępu do usług internetowych oraz naszych obiektów, prowadzenia dokumentacji działalności, przeprowadzania audytów, prowadzenia księgowości, analiz finansowych i ekonomicznych, realizacji płatności oraz związanych z nimi czynności księgowych, oceny ryzyka oraz zdolności kredytowej (scoring) itp.); **(b) zarządzania bezpieczeństwem i jego zapewniania** (*np.* ochrony infrastruktury IT, sprzętu biurowego oraz innego mienia); **(c) zarządzania działalnością operacyjną** (*np.* prowadzenia ewidencji danych przedstawicieli spółek i innych osób kontaktowych, zapewniania spójności działań pomiędzy różnymi jurysdykcjami, prowadzenia rejestrów spotkań i innych relacji biznesowych, obsługi systemów IT i systemów komunikacji oraz zarządzania nimi, zarządzania rozwojem i doskonaleniem produktów i usług, zarządzania majątkiem spółki, planowania strategicznego, zarządzania projektami, zapewniania ciągłości działania, tworzenia ścieżek audytowych i innych narzędzi sprawozdawczych itp.); **(d) wywiązywania się z obowiązków wynikających z obowiązujących przepisów prawa** (*np.* obowiązków w zakresie ochrony danych osobowych i podatków, wymogów MiFID dotyczących odpowiedniości i adekwatności produktów inwestycyjnych, przeciwdziałania nadużyciom i praniu pieniędzy, prowadzenia wymaganej dokumentacji i sprawozdawczości, dochodzenia praw i roszczeń, obrony w sporach i postępowaniach sądowych, zapewnienia zgodności z kontrolami prowadzonymi przez organy administracji publicznej oraz realizacji innych żądań właściwych organów, udzielania odpowiedzi na wezwania i inne czynności procesowe itp.); oraz **(e) planowania i realizacji strategii lub kampanii marketingowych** *(np.* prowadzenia badań marketingowych, planowania kampanii i opracowywania strategii marketingowych, monitorowania skuteczności kampanii i sporządzania sprawozdań na ten temat, kierowania ofert produktów i usług do określonych odbiorców, w tym profilowania, za zgodą osoby, której dane dotyczą, lub gdy jest to dozwolone przez prawo itp.).

W odniesieniu do **szczególnych kategorii danych osobowych klientów i kontrahentów (w tym ich pracowników, przedstawicieli i/lub agentów), w tym, o ile jest to dopuszczalne,** danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych, dane te mogą być przetwarzane przez Członków Grupy, jeżeli jest to niezbędne do realizacji celów określonych w niniejszej Polityce (*np.* wywiązywania się z obowiązków prawnych, identyfikowania publicznie dostępnych informacji dotyczących działalności klientów lub innych podmiotów, które mogą mieć wpływ na relacje ze spółką, zapewnienia spójności informacji pomiędzy różnymi jurysdykcjami, zapewnienia zgodności z kontrolami prowadzonymi przez organy administracji publicznej lub sądy oraz realizacji innych żądań właściwych organów itp.), wyłącznie w zakresie niezbędnym do wykonywania obowiązków Członków Grupy lub osoby, której dane dotyczą, w obszarze przeciwdziałania praniu pieniędzy, przeciwdziałania nadużyciom, zapobiegania przestępczości oraz w obszarach pokrewnych, jeżeli jest to wymagane lub dozwolone przez obowiązujące przepisy prawa.

- Przekazywanie danych osobowych **potencjalnych i obecnych dostawców oraz usługodawców** (w tym ich pracowników, przedstawicieli i/lub agentów) odbywa się w następujących celach: **(a) zarządzania relacją (przed)umowną z nimi lub reprezentowaną przez nich spółką (w przypadku osób prawnych)** (*np.* weryfikacji spełniania standardów jakości, analizy poziomu ryzyka dostawców, prowadzenia księgowości, analiz finansowych i ekonomicznych, podejmowania działań poprzedzających zawarcie odpowiednich umów, wykonywania zawartych umów, realizacji płatności oraz związanych z nimi czynności księgowych, na potrzeby prowadzenia działalności gospodarczej i komunikacji biznesowej, nawiązywania, odnawiania, utrzymywania i rozwiązywania relacji biznesowych oraz prowadzenia dokumentacji działalności); **(b) zapewniania bezpieczeństwa** (*np.* ochrony infrastruktury IT, sprzętu biurowego oraz innego mienia); **(c) zarządzania działalnością operacyjną** (*np.* obsługi i zarządzania systemami IT oraz systemami komunikacji, zarządzania rozwojem oraz doskonaleniem produktów i usług, planowania strategicznego, zarządzania projektami, zapewniania ciągłości działania, tworzenia ścieżek audytowych i innych narzędzi sprawozdawczych,

prowadzenia dokumentacji działalności, budżetowania, zarządzania finansami i sprawozdawczości oraz komunikacji); oraz **(d) wywiązywania się z obowiązków wynikających z obowiązujących przepisów prawa** (*np.* przepisów prawa handlowego, podatkowego, obowiązków w zakresie przeciwdziałania nadużyciom, obowiązków związanych z outsourcingiem przez podmioty finansowe, przeprowadzania audytów, zapewnienia zgodności z wymogami wynikającymi z kontroli prowadzonych przez organy administracji publicznej oraz realizacji innych żądań właściwych organów, dochodzenia praw i roszczeń, obrony w postępowaniach sądowych oraz rozpatrywania wewnętrznych skarg i roszczeń).

- Przekazywanie danych osobowych **akcjonariuszy** odbywa się w celu: **(a) zarządzania relacją z akcjonariuszem** (*np.* na potrzeby prowadzenia działalności gospodarczej i komunikacji biznesowej, nawiązywania, odnawiania, utrzymywania i rozwiązywania relacji z akcjonariuszami, organizacji walnych zgromadzeń oraz wykonywania praw akcjonariuszy, wypłaty dywidend, prowadzenia dokumentacji działalności, zapewniania dostępu do usług internetowych oraz do obiektów); oraz (**b) wywiązywania się z obowiązków wynikających z obowiązujących przepisów prawa** (*np.* przepisów prawa handlowego i prawa spółek, przepisów podatkowych oraz dotyczących papierów wartościowych, przeprowadzania audytów, zapewnienia zgodności z wymogami wynikającymi z kontroli prowadzonych przez organy administracji publicznej oraz realizacji innych żądań właściwych organów, wykonywania obowiązków w zakresie przeciwdziałania praniu pieniędzy, wydawania i uzyskiwania wymaganych poświadczeń, dochodzenia praw i roszczeń, obrony w postępowaniach sądowych oraz rozpatrywania wewnętrznych skarg i roszczeń).

- Przekazywanie danych osobowych **użytkowników stron internetowych, użytkowników końcowych oraz użytkowników instytucjonalnych (w tym użytkowników platform, stron internetowych i aplikacji związanych z uczelniami, zatrudnieniem oraz przedsiębiorczością)** odbywa się w celu: **(a) zarządzania świadczeniem usług** (*np.* opracowywania i udostępniania funkcji i treści dostępnych online, zarządzania stronami internetowymi, obsługi zapytań i wniosków oraz zapewniania wsparcia); **(b) zapewniania bezpieczeństwa** (*np.* ochrony infrastruktury IT oraz zapewniania bezpieczeństwa i integralności systemów, serwerów i stron internetowych); **(c) zarządzania działalnością operacyjną** (*np.* zapewniania spójności działań pomiędzy różnymi jurysdykcjami, prowadzenia rejestrów spotkań i innych relacji biznesowych oraz usprawniania globalnych procesów z zakresu zarządzania personelem i pozyskiwania talentów); **(d) planowania i realizacji strategii lub kampanii marketingowych** (*np.* prowadzenia badań marketingowych, planowania kampanii i opracowywania strategii marketingowych, monitorowania i raportowania skuteczności kampanii, kierowania ofert produktów i usług do określonych odbiorców (w tym profilowania), za zgodą osoby, której dane dotyczą, lub gdy jest to dozwolone przez prawo); **(e) prowadzenia krajowych i międzynarodowych procesów rekrutacyjnych** (*np.* oceny kandydatur i podejmowania decyzji o zatrudnieniu oraz komunikacji z kandydatami w związku z procesem rekrutacji lub złożonymi zgłoszeniami); **(f) prowadzenia zagregowanych analiz i segmentacji oraz sporządzania statystyk i analiz** (*np.* analizy sposobu korzystania z usług, doskonalenia i rozwijania funkcjonalności stron internetowych i usług oraz poprawy ich wydajności i jakości wsparcia); oraz **(g) wywiązywania się z obowiązków wynikających z obowiązujących przepisów prawa** (*np.* przepisów prawa handlowego, przeprowadzania audytów, zapewnienia zgodności z wymogami wynikającymi z kontroli prowadzonych przez organy administracji publicznej oraz realizacji innych żądań właściwych organów, udzielania odpowiedzi na wezwania i inne czynności procesowe, dochodzenia praw i roszczeń, obrony w postępowaniach sądowych oraz rozpatrywania wewnętrznych skarg i roszczeń).

Dane osobowe objęte niniejszą Polityką są również przekazywane pomiędzy Członkami Grupy w zakresie **niezbędnym do świadczenia na ich rzecz szerokiego zakresu usług wewnętrznych** (*np.* usług IT, usług back-office, rekrutacji i zarządzania personelem, audytu wewnętrznego i compliance, obsługi kanału zgłaszania nieprawidłowości, centralnej obsługi korespondencji dotyczącej wniosków i pracowników, technologii płatniczych i usług przetwarzania płatności, usług autoryzacji i rozliczania transakcji kartowych, usług

fakturowania i kalkulacji cen, niszczenia dokumentów, transportu dokumentów, zarządzania ryzykiem, zakupów produktów i usług, fakturowania elektronicznego, zarządzania marketingiem i komunikacją, a także usług prawnych i koordynacji prawnej w określonych obszarach, takich jak ochrona danych osobowych itp.).

DALSZE INFORMACJE

Grupa Santander wyznaczyła lokalnych Inspektorów Ochrony Danych (IOD) i/lub Championów (zgodnie z definicjami przedstawionymi poniżej), którzy kierują lokalnymi zespołami, zapewniają zgodność z przepisami na poziomie lokalnym w poszczególnych podmiotach na całym świecie oraz wchodzą w skład Zespołu ds. Prywatności Grupy Santander (zgodnie z definicją przedstawioną poniżej). Jeżeli mają Państwo jakiekolwiek pytania dotyczące postanowień niniejszej Polityki, praw przysługujących Państwu na jej podstawie lub innych kwestii związanych z ochroną danych osobowych, mogą Państwo skontaktować się z właściwym Inspektorem Ochrony Danych (IOD) lub Championem pod adresem wskazanym poniżej. Inspektor Ochrony Danych (IOD) lub Champion zajmie się sprawą, przekaże ją właściwej osobie lub jednostce organizacyjnej w Grupie Santander albo, w stosownych przypadkach, skieruje ją do właściwej osoby lub właściwego organu.

Adresat: Zespół ds. Prywatności

E-mail: Lista odpowiednich adresów e-mail jest dostępna tutaj.

Jeżeli mają Państwo jakiekolwiek wątpliwości dotyczące sposobu, w jaki którykolwiek Członek Grupy przetwarzał Państwa dane osobowe, mogą Państwo skorzystać z odrębnej procedury rozpatrywania skarg określonej w Części III (zob. **Załącznik 2**).

CZĘŚĆ II: OBOWIĄZKI CZŁONKÓW GRUPY

Część II niniejszej Polityki została podzielona na trzy sekcje.

- Sekcja A określa podstawowe zasady ochrony danych zgodne z europejskim prawem ochrony danych, których Członkowie Grupy są zobowiązani przestrzegać.

- Sekcja B dotyczy praktycznych zobowiązań podjętych przez Członków Grupy wobec właściwych organów nadzorczych w związku z niniejszą Polityką.

- Sekcja C opisuje prawa osób trzecich będących beneficjentami, przyznane osobom, których dane dotyczą, przez Członków Grupy na podstawie Części II niniejszej Polityki.

SEKCJA A: PODSTAWOWE ZASADY

ZASADA 1 - ZGODNOŚĆ Z PRAWEM I RZETELNOŚĆ

Zasada 1A - Członkowie Grupy będą przestrzegać niniejszej Polityki oraz wszelkich mających zastosowanie lokalnych przepisów o ochronie danych osobowych w sposób zapewniający ich spójne stosowanie.

Jako organizacje Członkowie Grupy, z zastrzeżeniem poniższych postanowień, będą przestrzegać wszelkich obowiązujących przepisów dotyczących danych osobowych (*np.* w Europie - europejskiego prawa ochrony danych) oraz zapewnią, że dane osobowe będą przetwarzane zgodnie z niniejszą Polityką oraz właściwym lokalnym prawem ochrony danych.

W przypadku gdy niniejsza Polityka ma zastosowanie oraz:

- jeżeli nie istnieje właściwe lokalne prawo ochrony danych lub prawo to nie spełnia standardów określonych w Zasadach niniejszej Polityki, Członkowie Grupy będą przetwarzać dane osobowe objęte niniejszą Polityką zgodnie z Zasadami określonymi w niniejszej Polityce;

- jeżeli właściwe lokalne prawo ochrony danych wymaga wyższego poziomu ochrony niż przewidziany w niniejszej Polityce, wyższy poziom ochrony ma pierwszeństwo przed niniejszą Polityką, pod warunkiem że prawa i obowiązki wynikające z niniejszej Polityki nadal są przestrzegane; lub

- jeżeli właściwe lokalne prawo ochrony danych uniemożliwia Członkom Grupy wywiązanie się z obowiązków wynikających z niniejszej Polityki lub w istotny sposób wpływa na ich zdolność do wywiązania się z tych obowiązków, Członkowie Grupy będą postępować zgodnie z procedurą określoną w Zasadzie 13.

Zasada 1B - Członkowie Grupy zapewnią, że przetwarzanie przez nie danych osobowych będzie zgodne z prawem i rzetelne oraz że, w przypadkach gdy jest to wymagane, istnieje podstawa prawna przetwarzania danych osobowych.

Członkowie Grupy zapewnią, że przetwarzanie danych osobowych przez nie będzie zgodne z prawem i rzetelne oraz że, w przypadkach gdy jest to wymagane, istnieje podstawa prawna przetwarzania danych osobowych. Zgodnie z europejskim prawem ochrony danych Członkowie Grupy będą przetwarzać dane osobowe wyłącznie wtedy, gdy:

- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych, a zgoda ta spełnia wymagane standardy wynikające z europejskiego prawa ochrony danych (tj. musi być dobrowolna, konkretna, świadoma i jednoznaczna); lub

- jest to niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy; lub

- jest to niezbędne do wypełnienia obowiązku prawnego, któremu podlega Członek Grupy (pod warunkiem, że takie prawo spełnia wymagania określone w Zasadzie 13 poniżej, w stosownych przypadkach); lub

- jest to niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; lub

- jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Członkowi Grupy (pod warunkiem, że takie zadanie zostało ustanowione prawem spełniającym wymagania określone w Zasadzie 13 poniżej, w stosownych przypadkach); lub

- jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Członka Grupy lub stronę trzecią, chyba że nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.

Jeżeli przetwarzanie danych osobowych dotyczy wyroków skazujących oraz czynów zabronionych lub związanych z nimi środków bezpieczeństwa, Członkowie Grupy nie będą przetwarzać takich danych inaczej niż pod kontrolą władz publicznych lub gdy przetwarzanie jest dozwolone przez prawo przewidujące odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą, zgodnie z powyższymi podstawami prawnymi.

Zasada 1C - Z zastrzeżeniem postanowień Zasady 1B, przetwarzanie szczególnych kategorii danych osobowych jest zabronione, chyba że ma zastosowanie jedno z odstępstw przewidzianych w europejskim prawie ochrony danych.

Przetwarzanie szczególnych kategorii danych osobowych jest dozwolone wyłącznie na określonych podstawach:

- Członek Grupy uzyskał wyraźną zgodę na przetwarzanie szczególnych kategorii danych osobowych dotyczących osoby, której dane dotyczą, w jednym lub kilku określonych celach, chyba że prawo stanowi, iż zakaz przetwarzania szczególnych kategorii danych osobowych nie może zostać uchylony przez osobę, której dane dotyczą; lub

- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw Członka Grupy lub osoby, której dane dotyczą, w dziedzinie prawa pracy oraz prawa zabezpieczenia społecznego i ochrony socjalnej, w zakresie, w jakim jest to dozwolone przez prawo lub układ zbiorowy zawarty na podstawie prawa przewidującego odpowiednie zabezpieczenia praw podstawowych i interesów osób, których dane dotyczą; lub

- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub

- przetwarzanie jest prowadzone, w ramach zgodnej z prawem działalności, z odpowiednimi zabezpieczeniami, przez fundację, stowarzyszenie lub inny podmiot nienastawiony na zysk o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu albo osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą; lub

- przetwarzanie dotyczy danych osobowych, które zostały w sposób oczywisty upublicznione przez osobę, której dane dotyczą; lub

- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub gdy sądy działają w ramach sprawowania wymiaru sprawiedliwości; lub

- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa, które jest proporcjonalne do zamierzonego celu, szanuje istotę prawa do ochrony danych oraz przewiduje odpowiednie i szczególne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą; lub

- przetwarzanie jest niezbędne do celów medycyny zapobiegawczej lub medycyny pracy, oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub społecznej bądź leczenia albo zarządzania systemami i usługami opieki zdrowotnej lub społecznej, na podstawie prawa, pod warunkiem że przetwarzanie jest dokonywane przez osobę wykonującą zawód podlegający obowiązkowi zachowania tajemnicy zawodowej lub pod jej odpowiedzialnością, zgodnie z prawem lub zasadami ustanowionymi przez właściwe organy krajowe; lub

- przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, na podstawie prawa przewidującego odpowiednie i szczególne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności obowiązek zachowania tajemnicy zawodowej; lub

- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, badań naukowych lub historycznych albo do celów statystycznych, na podstawie prawa, które jest proporcjonalne do zamierzonego celu, szanuje istotę prawa do ochrony danych oraz przewiduje odpowiednie i szczególne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Zasada 1D - Członkowie Grupy przeprowadzą ocenę skutków każdego przetwarzania danych osobowych, które będzie wiązało się z wysokim ryzykiem dla praw i wolności osób, których dane dotyczą.

Podmioty Eksportujące, działając jako administratorzy danych, ocenią niezbędność i proporcjonalność każdego nowego procesu przetwarzania danych osobowych, a w przypadku gdy będzie się on wiązał z wysokim ryzykiem dla praw i wolności osób, których dane dotyczą, przeprowadzą ocenę skutków dla ochrony danych osobowych zgodnie z europejskim prawem ochrony danych. W przypadku gdy ocena skutków dla ochrony danych osobowych wykaże, że przetwarzanie będzie wiązało się z wysokim ryzykiem dla osób, których dane dotyczą, Podmioty Eksportujące skonsultują się z właściwym organem nadzorczym przed rozpoczęciem przetwarzania, jeżeli nie wdrożono środków ograniczających to ryzyko.

ZASADA 2 - ZAPEWNIENIE PRZEJRZYSTOŚCI ORAZ PRZETWARZANIE DANYCH OSOBOWYCH WYŁĄCZNIE W OKREŚLONYM CELU

Zasada 2A - Członkowie Grupy będą informować osoby, których dane dotyczą, o tym, w jaki sposób ich dane będą przetwarzane.

Członkowie Grupy zapewnią, że osoby, których dane dotyczą, są zawsze informowane w sposób jasny i wyczerpujący (zwykle za pomocą klauzuli informacyjnej) o tym, w jaki sposób ich dane osobowe będą przetwarzane. Właściwy Członek Grupy przekaże informacje zgodne z wymogami europejskiego prawa ochrony danych, obejmujące co najmniej następujące informacje:

- tożsamość i dane kontaktowe administratora, w tym dane kontaktowe Inspektora Ochrony Danych (IOD) oraz przedstawiciela, w stosownych przypadkach;
- cel i podstawę prawną przetwarzania, w tym wyjaśnienie dotyczące wszelkiego przetwarzania opartego na prawnie uzasadnionych interesach oraz wszelkich nowych lub innych zgodnych celów;
- odbiorców lub kategorie odbiorców danych osobowych;
- informacje na temat wdrożonych zabezpieczeń służących ochronie danych osobowych w związku z ich międzynarodowym przekazywaniem oraz sposobu uzyskania dostępu do tych zabezpieczeń lub otrzymania ich kopii. W przypadku przekazywania danych osobowych między Podmiotem Eksportującym a Podmiotem Importującym na podstawie niniejszej Polityki przekazywane informacje będą zawierać odniesienie do niniejszej Polityki oraz informację o sposobie uzyskania do niej dostępu;
- okres, przez który dane osobowe będą przechowywane, lub kryteria stosowane do ustalenia tego okresu;
- informacje o prawach osoby, której dane dotyczą, w tym o prawie dostępu do danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu, przenoszenia danych, prawie do wycofania zgody (jeżeli przetwarzanie odbywa się na podstawie zgody) oraz prawie wniesienia skargi do właściwego organu nadzorczego;
- czy podanie danych osobowych jest wymogiem ustawowym lub umownym oraz jakie są konsekwencje niepodania danych osobowych; oraz
- informacje o istnieniu zautomatyzowanego podejmowania decyzji, w tym profilowania, a co najmniej w przypadkach, gdy takie decyzje wywołują wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływają albo są oparte na szczególnych kategoriach danych osobowych, istotne informacje o zastosowanej logice, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Wymogi właściwego lokalnego prawa ochrony danych obowiązującego w państwie, w którym dane osobowe są zbierane, określą, czy osobom, których dane dotyczą, należy przekazać dodatkowe informacje.

Informacje te zostaną przekazane w momencie pozyskania przez Członków Grupy danych osobowych od osoby, której dane dotyczą, lub w innym terminie dozwolonym na mocy europejskiego prawa ochrony danych.

Jeżeli Członkowie Grupy pozyskują dane osobowe osoby, której dane dotyczą, ze źródła innego niż ta osoba, właściwy Członek Grupy przekaże te informacje osobie, której dane dotyczą, wraz z informacjami o źródle danych oraz kategoriach pozyskanych danych osobowych, w następujących terminach:

- w rozsądnym terminie po pozyskaniu danych osobowych, jednak nie później niż w ciągu jednego (1) miesiąca;
- jeżeli dane osobowe mają być wykorzystywane do kontaktu z osobą, której dane dotyczą, najpóźniej przy pierwszym kontakcie z tą osobą; lub
- jeżeli dane mają zostać ujawnione osobie trzeciej, nie później niż w chwili ich pierwszego ujawnienia.

Członkowie Grupy będą przestrzegać niniejszej Zasady 2A, chyba że nieprzekazanie tych informacji jest wyraźnie dozwolone na mocy europejskiego prawa ochrony danych.

Zasada 2B - Członkowie Grupy będą pozyskiwać i przetwarzać dane osobowe wyłącznie w celach znanych osobie, której dane dotyczą, lub zgodnych z uzasadnionymi oczekiwaniami osoby, której dane dotyczą, oraz istotnych dla Członków Grupy.

Zasada 1A stanowi, że Członkowie Grupy będą przestrzegać wszelkich mających zastosowanie przepisów prawa dotyczących przetwarzania danych osobowych (pod warunkiem że przepisy te spełniają wymagania określone w Zasadzie 13, w stosownych przypadkach). Oznacza to, że Członkowie Grupy będą zbierać dane osobowe w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nie będą dalej przetwarzać tych danych osobowych w sposób niezgodny z tymi celami.

Członkowie Grupy określą i podadzą do wiadomości cele, w jakich dane osobowe będą przetwarzane (w tym dalsze sposoby wykorzystania danych oraz ich ujawniania), zgodnie z Zasadą 2A.

Zasada 2C - Członkowie Grupy mogą przetwarzać dane osobowe w innym lub nowym celu wyłącznie wtedy, gdy jest on zgodny z celem, w jakim dane zostały zebrane.

Jeżeli Członek Grupy zbiera dane osobowe w określonym celu zgodnie z Zasadą 2A (zgodnie z informacjami przekazanymi osobie, której dane dotyczą, w odpowiedniej klauzuli informacyjnej) oraz zgodnie z opisem zawartym w Zasadzie 2B, a następnie zamierza przetwarzać dane osobowe w innym lub nowym celu, nie będzie dalej przetwarzać tych danych osobowych w sposób niezgodny z celem, w jakim zostały zebrane, chyba że takie dalsze przetwarzanie opiera się na zgodzie osoby, której dane dotyczą, lub jest wymagane przez prawo (pod warunkiem że prawo to spełnia wymagania określone w Zasadzie 13, w stosownych przypadkach).

ZASADA 3 - ZAPEWNIENIE JAKOŚCI DANYCH

Zasada 3A - Członkowie Grupy będą utrzymywać dane osobowe prawidłowe i aktualne.

W celu zapewnienia, aby dane osobowe posiadane przez Członków Grupy były prawidłowe i aktualne, Członkowie Grupy będą zachęcać osoby, których dane dotyczą, do informowania ich, gdy ich dane osobowe ulegną zmianie. Członkowie Grupy podejmą wszelkie rozsądne działania w celu zapewnienia, aby dane osobowe nieprawidłowe w świetle celów, w jakich są przetwarzane, zostały niezwłocznie usunięte lub sprostowane.

Zasada 3B - Członkowie Grupy będą przechowywać dane osobowe wyłącznie tak długo, jak jest to niezbędne do celów, w jakich są przetwarzane.

Członkowie Grupy będą przestrzegać przepisów mających zastosowanie do każdego Członka Grupy oraz polityk i procedur Grupy Santander dotyczących retencji dokumentacji, okresowo zmienianych i aktualizowanych. Oznacza to między innymi, że Członkowie Grupy będą usuwać lub blokować, w zależności od okoliczności, dane osobowe, które nie są już niezbędne do celów, w jakich zostały zebrane i są dalej przetwarzane.

Zasada 3C - Członkowie Grupy będą przetwarzać wyłącznie dane osobowe, które są adekwatne, stosowne i ograniczone do tego, co jest niezbędne do celów, w jakich są przetwarzane.

Członkowie Grupy będą przetwarzać wyłącznie dane osobowe adekwatne, stosowne i ograniczone do tego, co jest niezbędne do realizacji celów, w jakich są przetwarzane.

ZASADA 4 - PODEJMOWANIE ODPOWIEDNICH ŚRODKÓW BEZPIECZEŃSTWA

Zasada 4A - Członkowie Grupy będą przestrzegać polityk bezpieczeństwa IT Grupy Santander.

Członkowie Grupy wdrożą odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem lub utratą, zmianą, nieuprawnionym ujawnieniem lub dostępem, w szczególności gdy przetwarzanie obejmuje przekazywanie danych osobowych za pośrednictwem sieci, a także przed wszelkimi innymi niezgodnymi z prawem formami przetwarzania. W tym celu Członkowie Grupy będą przestrzegać wymagań określonych w politykach bezpieczeństwa obowiązujących w Grupie Santander, okresowo przeglądanych i aktualizowanych, a także wszelkich innych procedur bezpieczeństwa właściwych dla danego obszaru działalności lub funkcji. Uwzględniając stan wiedzy technicznej oraz koszty wdrożenia, środki te zapewniają poziom bezpieczeństwa odpowiedni do ryzyka wynikającego z przetwarzania oraz charakteru danych podlegających ochronie.

Zasada 4B - Członkowie Grupy wdrożyli politykę powiadamiania o naruszeniach ochrony danych.

Członkowie Grupy wdrożyli procedury reagowania na naruszenia ochrony danych osobowych (okresowo zmieniane i aktualizowane), które określają proces postępowania w przypadku naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych („**naruszenie ochrony danych osobowych**").

W szczególności w przypadku naruszenia ochrony danych osobowych osoba, która w ramach danego Członka Grupy poweźmie wiadomość o naruszeniu, bez zbędnej zwłoki zgłosi je:

- właściwemu Inspektorowi Ochrony Danych (IOD) lub Championowi, za pośrednictwem Funkcji Kontroli Ryzyka Operacyjnego (w stosownych przypadkach);
- Członkowi Grupy działającemu jako administrator danych, gdy dany Członek Grupy działa jako podmiot przetwarzający; oraz
- Odpowiedzialnemu Członkowi BCR.

Właściwy Inspektor Ochrony Danych (IOD) lub Champion oceni, w razie potrzeby przy wsparciu Korporacyjnego Biura ds. Ochrony Danych, czy naruszenie ochrony danych osobowych powinno zostać zgłoszone właściwemu organowi nadzorczemu. W takim przypadku właściwy Inspektor Ochrony Danych

(IOD) lub Champion, w zależności od sytuacji, zgłosi naruszenie ochrony danych osobowych właściwemu organowi nadzorczemu w wymaganym terminie (zgodnie z europejskim prawem ochrony danych, bez zbędnej zwłoki oraz, w miarę możliwości, nie później niż w ciągu 72 godzin od stwierdzenia naruszenia).

Osoby, których dane dotyczą, zostaną również powiadomione bez zbędnej zwłoki w przypadkach, gdy naruszenie ochrony danych osobowych prawdopodobnie będzie wiązać się z wysokim ryzykiem dla ich praw i wolności, chyba że taki obowiązek nie wynika z europejskiego prawa ochrony danych.

Zgodnie z powyższym naruszenia ochrony danych osobowych, do których doszło u Członków Grupy, obejmujące informacje o okolicznościach naruszenia, jego skutkach oraz podjętych działaniach naprawczych, będą również rejestrowane w systemie Heracles, stanowiącym rejestr incydentów bezpieczeństwa Grupy Santander (w tym naruszeń ochrony danych osobowych), który będzie udostępniany właściwemu organowi nadzorczemu na jego żądanie.

Zasada 4C - Członkowie Grupy zapewnią, że dostawcy usług oraz inne podmioty przetwarzające dane osobowe w ich imieniu również wdrożą odpowiednie i równoważne środki bezpieczeństwa.

Członkowie Grupy korzystający z usług usługodawcy (działającego jako podmiot przetwarzający), który ma dostęp do danych osobowych osób, których dane dotyczą (*np.* dostawcy usług płacowych), zawrą z podmiotem przetwarzającym pisemną umowę powierzenia przetwarzania danych spełniającą wymogi europejskiego prawa ochrony danych. Przedmiotowa umowa powinna co najmniej zawierać następujące postanowienia:

- Przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą;
- Obowiązki i prawa administratora;
- Następujące obowiązki podmiotu przetwarzającego:
    - Przetwarzać dane osobowe wyłącznie na udokumentowane polecenie administratora, w tym w odniesieniu do przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, chyba że taki obowiązek wynika z prawa, któremu podlega podmiot przetwarzający (pod warunkiem że prawo to spełnia wymogi określone w Zasadzie 13, w stosownych przypadkach). W takim przypadku podmiot przetwarzający informuje administratora o tym obowiązku prawnym przed rozpoczęciem przetwarzania, chyba że prawo to zabrania przekazania takich informacji z ważnych względów interesu publicznego;
    - Zapewnić, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności;
    - Wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiedni do ryzyka związanego z przetwarzaniem danych osobowych;
    - Nie korzystać z usług dalszego podmiotu przetwarzającego w związku z przetwarzaniem danych osobowych bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora oraz, w stosownych przypadkach, zawrzeć z dalszym podmiotem przetwarzającym umowę na piśmie, nakładającą na niego takie same obowiązki w zakresie ochrony danych, jakie określono w umowie lub innym akcie prawnym zawartym między administratorem a podmiotem przetwarzającym (w szczególności zapewniającą wystarczające gwarancje

wdrożenia odpowiednich środków technicznych i organizacyjnych w taki sposób, aby przetwarzanie spełniało wymagania europejskiego prawa ochrony danych);

- Uwzględniając charakter przetwarzania, pomagać administratorowi, w miarę możliwości, za pomocą odpowiednich środków technicznych i organizacyjnych, w wywiązywaniu się z obowiązku odpowiadania na żądania dotyczące wykonywania praw osoby, której dane dotyczą (szczegółowo opisanych w Zasadzie 5);

- Pomagać administratorowi w zapewnieniu zgodności z obowiązkami dotyczącymi wdrażania odpowiednich środków bezpieczeństwa, przeprowadzania ocen skutków dla ochrony danych osobowych oraz związanych z nimi konsultacji z właściwymi organami nadzorczymi, a także wywiązywania się z obowiązków zgłaszania naruszeń ochrony danych osobowych właściwym organom nadzorczym oraz osobom, których dane dotyczą (w stosownych przypadkach);

- Zgodnie z wyborem administratora usunąć lub zwrócić administratorowi wszystkie dane osobowe po zakończeniu świadczenia usług związanych z przetwarzaniem oraz usunąć istniejące kopie, chyba że przechowywanie danych osobowych jest wymagane przez prawo;

- Udostępniać administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków podmiotu przetwarzającego oraz umożliwiać przeprowadzanie audytów, w tym inspekcji, oraz współpracować przy ich prowadzeniu, prowadzonych przez administratora lub innego audytora upoważnionego przez administratora; oraz

- Niezwłocznie poinformować administratora, jeżeli w ocenie podmiotu przetwarzającego polecenie narusza prawo.

ZASADA 5 - POSZANOWANIE PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

Zasada 5 - Członkowie Grupy będą rozpatrywać żądania osób, których dane dotyczą, dotyczące wykonywania przysługujących im praw w zakresie ochrony danych osobowych (w tym prawa dostępu do danych osobowych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych osobowych, wniesienia sprzeciwu wobec przetwarzania danych osobowych oraz wycofania zgody).

Na wniosek osoby, której dane dotyczą, osobie tej przysługują następujące prawa przewidziane w europejskim prawie ochrony danych:

- prawo dostępu, obejmujące przekazanie informacji o danych osobowych dotyczących osoby, której dane dotyczą, oraz potwierdzenie czy dane osobowe tej osoby są przetwarzane;

- prawo do sprostowania, zgodnie z którym osoba, której dane dotyczą, ma prawo uzyskać sprostowanie wszelkich danych osobowych, które są nieprawidłowe lub niekompletne;

- prawo do usunięcia danych („prawo do bycia zapomnianym”), zgodnie z którym osoba, której dane dotyczą, ma prawo żądać usunięcia swoich danych osobowych w przypadkach określonych w art. 17 RODO;

- prawo do ograniczenia przetwarzania, zgodnie z którym osoba, której dane dotyczą, ma prawo żądać ograniczenia przetwarzania swoich danych osobowych w przypadkach określonych w art. 18 RODO;

- prawo do tego, aby każdy odbiorca, któremu ujawniono dane osobowe, został powiadomiony o sprostowaniu lub usunięciu danych osobowych albo o ograniczeniu przetwarzania, chyba że okaże się to niemożliwe lub będzie wymagało niewspółmiernie dużego wysiłku. Osoba, której dane dotyczą, może również zażądać informacji o tych odbiorcach;

- prawo do przenoszenia danych, zgodnie z którym osoba, której dane dotyczą, ma prawo otrzymać dotyczące jej dane osobowe, które dostarczyła administratorowi, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego oraz przesłać te dane innemu administratorowi;

- prawo do wniesienia sprzeciwu, zgodnie z którym osoba, której dane dotyczą, ma prawo sprzeciwić się przetwarzaniu swoich danych osobowych w określonym celu, w tym przetwarzaniu do celów marketingu bezpośredniego oraz profilowaniu w zakresie, w jakim jest ono związane z takim marketingiem;

- prawo do tego, aby nie podlegać decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, która wywołuje wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływa (w stosownych przypadkach); oraz

- prawo do wycofania zgody udzielonej na określone przetwarzanie w dowolnym momencie.

ZASADA 6 - ZAPEWNIENIE ODPOWIEDNIEGO POZIOMU OCHRONY PRZY PRZEKAZYWANIU I DALSZYM PRZEKAZYWANIU

Zasada 6 - Członkowie Grupy nie będą przekazywać danych osobowych podmiotom trzecim poza Europę bez zapewnienia odpowiedniej ochrony danych osobowych zgodnie ze standardami określonymi w niniejszej Polityce oraz zgodnie z europejskim prawem ochrony danych.

Przekazywanie i dalsze przekazywanie danych osobowych przez Członków Grupy podlegających europejskiemu prawu ochrony danych podmiotom trzecim spoza Europy jest niedozwolone bez podjęcia odpowiednich działań wymaganych przez europejskie prawo ochrony danych.

Działania te mogą obejmować między innymi:

- potwierdzenie, że podmiot trzeci ma siedzibę w państwie, wobec którego Komisja Europejska wydała decyzję stwierdzającą odpowiedni stopień ochrony przekazywanych danych osobowych; lub

- zawarcie odpowiednich standardowych klauzul umownych lub zastosowanie innych mechanizmów przewidzianych w europejskim prawie ochrony danych; lub

- gdy przekazanie jest konieczne w celu: (i) wykonania umowy zawartej między osobą, której dane dotyczą, a Członkiem Grupy dokonującym przekazania lub podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą; (ii) zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą, między Członkiem Grupy dokonującym przekazania a inną stroną; (iii) ważnych względów interesu publicznego uznanych w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator; (iv) ustalenia, dochodzenia lub obrony roszczeń; (v) ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub (vi) uzyskania wyraźnej zgody osoby, której dane dotyczą, po poinformowaniu jej o możliwym ryzyku takiego przekazania wynikającym z braku decyzji stwierdzającej odpowiedni stopień ochrony oraz odpowiednich zabezpieczeń.

SEKCJA B: PRAKTYCZNE ZOBOWIĄZANIA

ZASADA 7 - ZGODNOŚĆ I ODPOWIEDZIALNOŚĆ

Zasada 7A - Członkowie Grupy będą odpowiedzialni za przestrzeganie niniejszej Polityki oraz będą w stanie wykazać jej przestrzeganie, a także będą dysponować odpowiednim personelem i wsparciem w celu zapewnienia oraz nadzorowania przestrzegania niniejszej Polityki w całym przedsiębiorstwie.

Grupa Santander posiada strukturę organizacyjną ds. prywatności, odpowiedzialną za podejmowanie decyzji, koordynowanie, wdrażanie i nadzorowanie wszelkich kwestii dotyczących ochrony danych osobowych w ramach Grupy Santander („**Zespół ds. Prywatności**"). Struktura organizacyjna ds. prywatności Grupy Santander składa się z:

- **Korporacyjnego Biura ds. Ochrony Danych („Corporate DP Office"):** Korporacyjnego organu odpowiedzialnego za określanie ogólnych kryteriów oraz opracowywanie obowiązujących korporacyjnych polityk ochrony danych. Zostało ono utworzone wraz z Zespołem ds. Ryzyka Niefinansowego jako globalna druga linia obrony (2LoD), odpowiedzialna za nadzór nad zarządzaniem działaniami związanymi z prywatnością prowadzonymi przez pierwszą linię obrony (1LoD) oraz za zapewnienie odpowiedniego zarządzania ryzykiem zgodnie z apetytem na ryzyko Grupy Santander.

  Korporacyjne Biuro ds. Ochrony Danych oraz Zespół ds. Ryzyka Niefinansowego, jako globalna druga linia obrony (2LoD), pełnią szereg funkcji w odniesieniu do wszystkich podmiotów Grupy Santander podlegających europejskiemu prawu ochrony danych, w tym przede wszystkim:

  - Monitorowanie i kontrola zgodności: (i) nadzór nad zgodnością Grupy Santander z przepisami o ochronie danych osobowych; (ii) skonsolidowane raportowanie do najwyższego kierownictwa Grupy Santander; (iii) pełnienie funkcji globalnego punktu kontaktowego, za pośrednictwem lokalnych Inspektorów Ochrony Danych (IOD) (lub osób pełniących podobną funkcję), w relacjach z właściwymi organami nadzorczymi; (iv) analiza wpływu incydentów bezpieczeństwa na poziomie globalnym, prowadzona wspólnie z odpowiednimi funkcjami biznesowymi i wspierającymi; (v) globalna analiza ryzyka oraz raportowanie w zakresie ochrony danych osobowych; oraz (vi) wspieranie stosowania kryteriów korporacyjnych oraz pełnienie funkcji punktu kontaktowego dla Inspektorów Ochrony Danych (IOD) i Championów poszczególnych podmiotów (zob. poniżej).

  - Funkcja wspierająca Inspektorów Ochrony Danych (IOD) i Championów Grupy Santander (jednostek korporacyjnych, podmiotów Grupy oraz podmiotów lokalnych). Polega przede wszystkim na zapewnianiu specjalistycznego doradztwa w zakresie przepisów oraz wsparcia przy wykonywaniu lokalnych funkcji związanych z ochroną danych osobowych.

- **Struktura i ład korporacyjny**

  - **Banco Santander (korporacja)**: dwie główne funkcje wspierają Korporacyjne Biuro ds. Ochrony Danych i raportują do niego:

    - **Inspektor Ochrony Danych Banco Santander** (formalnie wyznaczony wobec hiszpańskiego organu nadzorczego): jego zadania w spółce dominującej, wykonywane niezależnie, ograniczają się do zadań określonych w RODO, które wymagają między

innymi jego udziału w kontaktach z hiszpańskim organem nadzorczym. Niezależnie od obowiązków Inspektora Ochrony Danych (IOD) w zakresie raportowania i wsparcia na rzecz Korporacyjnego Biura ds. Ochrony Danych, Inspektor Ochrony Danych (IOD) podlega bezpośrednio najwyższemu szczeblowi kierownictwa Banco Santander.

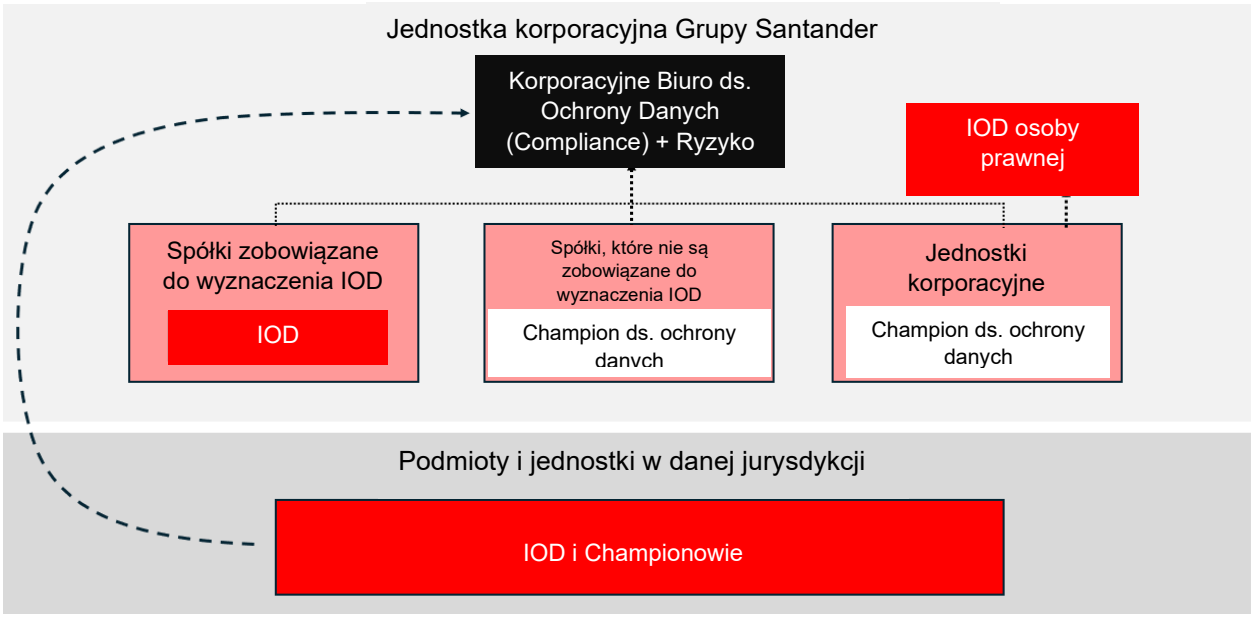
- **Jednostki korporacyjne**: jednostki wyznaczone w całej organizacji. Ich główne zadania i obowiązki obejmują: (a) prowadzenie i rozstrzyganie w pierwszej instancji spraw dotyczących danych osobowych; (b) informowanie i doradzanie administratorom, podmiotom przetwarzającym oraz pracownikom w zakresie przestrzegania obowiązujących przepisów o ochronie danych; (c) monitorowanie przestrzegania przepisów o ochronie danych; (d) pełnienie funkcji wewnętrznego punktu kontaktowego jako wsparcia pierwszego poziomu; (e) przekazywanie zapytań i wniosków o wsparcie do Korporacyjnego Biura ds. Ochrony Danych oraz raportowanie wskaźników zarządczych.

- **Jednostki lokalne**: istnieją również dwie funkcje raportujące do Korporacyjnego Biura ds. Ochrony Danych:

  - **Inspektorzy Ochrony Danych (IOD) (lub osoby pełniące podobną lokalną funkcję)**: jeżeli jest to wymagane przez właściwe lokalne prawo ochrony danych, wyznacza się Inspektora Ochrony Danych (IOD) (lub osobę pełniącą podobną lokalną funkcję). Ich główne zadania i obowiązki mogą obejmować: (a) pełnienie funkcji punktu kontaktowego dla właściwego organu nadzorczego oraz interesariuszy; (b) współpracę z właściwym organem nadzorczym; (c) doradztwo w zakresie ochrony danych osobowych; (d) monitorowanie i nadzór; (e) prowadzenie szkoleń; (f) doradztwo w zakresie ocen skutków dla ochrony danych osobowych; (g) prowadzenie uprzednich konsultacji z właściwym organem nadzorczym; (h) nadzorowanie prowadzenia rejestru czynności przetwarzania; (i) doradztwo w zakresie zgłaszania naruszeń ochrony danych osobowych; (j) doradztwo w zakresie zarządzania podmiotami trzecimi; oraz (k) nadzorowanie wykonywania praw osób, których dane dotyczą.

  - **Championowie (lub osoby pełniące podobną lokalną funkcję, *np.* Privacy Officer):** jeżeli zgodnie z właściwym lokalnym prawem ochrony danych wyznaczenie Inspektora Ochrony Danych (IOD) nie jest wymagane albo gdy ze względu na wielkość lub stopień złożoności danego podmiotu konieczne jest wyznaczenie większej liczby Inspektorów Ochrony Danych (IOD) lub osób pełniących podobną funkcję, Korporacyjne Biuro ds. Ochrony Danych może być wspierane przez lokalnych Championów (lub osoby pełniące podobną funkcję, *np.* Privacy Officer), którzy również raportują do tego Biura. Ich zadania i obowiązki są zasadniczo takie same jak zadania i obowiązki Inspektorów Ochrony Danych (IOD) (lub osób pełniących podobną funkcję), z wyjątkiem kontaktów z organami nadzorczymi, w których nie uczestniczą.

Poniżej przedstawiono schemat ilustrujący strukturę organizacyjną oraz relacje pomiędzy opisanymi powyżej funkcjami odpowiedzialnymi za ochronę danych w Grupie Santander:



Zasada 7B - Członkowie Grupy wdrożą odpowiednie środki techniczne i organizacyjne zgodnie z zasadami ochrony danych w fazie projektowania oraz domyślnej ochrony danych, aby umożliwić i ułatwić przestrzeganie Polityki w praktyce.

Uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, Członkowie Grupy wdrożą odpowiednie środki techniczne i organizacyjne, które służą skutecznej realizacji zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych, zgodnie z wymogami europejskiego prawa ochrony danych. Członkowie Grupy uwzględnią takie środki podczas określania sposobów przetwarzania oraz w czasie samego przetwarzania, aby zapewnić ochronę przetwarzanych danych osobowych oraz zagwarantować, że domyślnie przetwarzane będą wyłącznie dane osobowe niezbędne do każdego konkretnego celu przetwarzania.

Zasada 7C - Członkowie Grupy przetwarzający dane osobowe będą prowadzić pisemny rejestr (w tym w formie elektronicznej) czynności przetwarzania oraz udostępniać go właściwym organom nadzorczym na ich żądanie.

Rejestry czynności przetwarzania prowadzone przez Członków Grupy działających jako administratorzy będą zawierać:

- nazwę i dane kontaktowe Członka Grupy oraz, jeżeli ma to zastosowanie, współadministratora, przedstawiciela administratora oraz Inspektora Ochrony Danych (IOD);
- cele przetwarzania danych osobowych;
- opis kategorii osób, których dane dotyczą, oraz kategorii przetwarzanych danych osobowych;
- kategorie odbiorców, którym dane osobowe ujawniono lub którym zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;

- informacje o państwie trzecim lub państwach trzecich, do których przekazywane są dane osobowe, w tym identyfikację tego państwa trzeciego lub organizacji międzynarodowej oraz dokumentację odpowiednich zabezpieczeń wdrożonych w związku z takim przekazywaniem (chyba że wobec danego państwa wydano decyzję stwierdzającą odpowiedni stopień ochrony zgodnie z europejskim prawem ochrony danych);

- w miarę możliwości okres przechowywania danych osobowych; oraz

- w miarę możliwości ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych w celu ochrony danych osobowych.

Rejestry czynności przetwarzania prowadzone przez Członków Grupy działających jako podmioty przetwarzające na rzecz Członka Grupy będącego administratorem będą zawierać:

- nazwę i dane kontaktowe Członka Grupy oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a także, w stosownych przypadkach, przedstawiciela administratora lub podmiotu przetwarzającego oraz Inspektora Ochrony Danych (IOD);

- kategorie czynności przetwarzania wykonywanych w imieniu każdego administratora;

- informacje o państwie trzecim lub państwach trzecich, do których przekazywane są dane osobowe, w tym identyfikację tego państwa trzeciego lub organizacji międzynarodowej oraz dokumentację odpowiednich zabezpieczeń wdrożonych w związku z takim przekazywaniem (chyba że wobec danego państwa wydano decyzję stwierdzającą odpowiedni stopień ochrony zgodnie z europejskim prawem ochrony danych); oraz

- w miarę możliwości ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych w celu ochrony danych osobowych.

Rejestry czynności przetwarzania prowadzone przez Członków Grupy muszą mieć formę pisemną, w tym elektroniczną, i będą udostępniane właściwym organom nadzorczym na ich żądanie.

ZASADA 8 - SZKOLENIE

Zasada 8 - Członkowie Grupy zapewnią odpowiednie szkolenia pracownikom, którzy mają stały lub regularny dostęp do danych osobowych i/lub są zaangażowani w przetwarzanie danych osobowych lub w opracowywanie narzędzi wykorzystywanych do przetwarzania takich danych osobowych.

Członkowie Grupy zapewnią odpowiednie i aktualne szkolenia pracownikom, którzy mają stały lub regularny dostęp do danych osobowych i/lub są zaangażowani w przetwarzanie takich danych osobowych lub w opracowywanie narzędzi wykorzystywanych do przetwarzania takich danych osobowych. Takie szkolenie będzie organizowane co najmniej raz na dwa lata i będzie obejmować m.in. procedury obsługi wniosków o dostęp do danych osobowych składanych przez organy publiczne.

ZASADA 9 - AUDYT

Zasada 9 - Członkowie Grupy będą przestrzegać Programu audytu określonego w Załączniku 1.

Członkowie Grupy będą przestrzegać Programu audytu poprzez przeprowadzanie regularnych audytów wewnętrznych oraz umożliwianie przeprowadzania audytów zewnętrznych, tam, gdzie jest to wymagane,

zgodnie z formalnym procesem oceny przewidzianym w Programie audytu. Wyniki takich audytów zostaną przekazane zgodnie z Załącznikiem 1.

ZASADA 10- ROZPATRYWANIE SKARG

Zasada 10 - Członkowie Grupy będą przestrzegać Procedury rozpatrywania skarg określonej w Załączniku 2.

Członkowie Grupy będą przestrzegać Procedury rozpatrywania skarg określonej w Załączniku 2 w celu należytego rozpatrywania skarg osób, których dane dotyczą, oraz zapewnienia bezpieczeństwa przetwarzania danych osobowych przez Członków Grupy. Członkowie Grupy umożliwią również wykonywanie praw osób trzecich będących beneficjentami określonych w sekcji C niniejszej Polityki.

ZASADA 11 - WSPÓŁPRACA Z WŁAŚCIWYMI ORGANAMI NADZORCZYMI

Zasada 11 - Członkowie Grupy będą przestrzegać Procedury współpracy określonej w Załączniku 3.

Członkowie Grupy będą przestrzegać Procedury współpracy określonej w Załączniku 3 oraz będą współpracować z właściwymi organami nadzorczymi w związku z niniejszą Polityką, w tym poddawać się przeprowadzanym przez nie audytom i kontrolom (w razie potrzeby również na miejscu), a także uwzględniać ich zalecenia oraz stosować się do ich decyzji we wszelkich sprawach związanych z niniejszą Polityką.

ZASADA 12 - AKTUALIZACJA POLITYKI

Zasada 12 - Członkowie Grupy będą przestrzegać Procedury aktualizacji określonej w Załączniku 4.

Członkowie Grupy będą przestrzegać Procedury aktualizacji określonej w Załączniku 4 oraz będą bez zbędnej zwłoki przekazywać informacje o wszelkich zmianach niniejszej Polityki oraz o zmianach listy Członków Grupy właściwym organom nadzorczym, osobom, których dane dotyczą, oraz Członkom Grupy, w zakresie, w jakim będzie to wymagane.

ZASADA 13 - POSTĘPOWANIE W PRZYPADKU, GDY PRAWO KRAJOWE UNIEMOŻLIWIA PRZESTRZEGANIE POLITYKI

Zasada 13A - Członkowie Grupy zobowiązują się stosować niniejszą Politykę jako podstawę przekazywania danych do Podmiotów Importujących wyłącznie po dokonaniu należytej oceny, że prawo i praktyki obowiązujące w kraju Podmiotów Importujących (w tym wszelkie wymogi dotyczące ujawniania danych osobowych lub środki upoważniające organy władzy publicznej do uzyskiwania do nich dostępu) nie uniemożliwiają im wywiązania się z obowiązków wynikających z niniejszej Polityki.

Członkowie Grupy będą stosować niniejszą Politykę jako podstawę międzynarodowego przekazywania danych osobowych wyłącznie wtedy, gdy ocenią, że prawo i praktyki obowiązujące w odpowiednich docelowych państwach trzecich, w tym wszelkie wymogi dotyczące ujawniania danych osobowych lub środki upoważniające organy władzy publicznej do uzyskiwania dostępu do danych osobowych, nie uniemożliwiają im wywiązania się z obowiązków wynikających z niniejszej Polityki. Ocena ta opiera się na założeniu, że przepisy prawa i praktyki, które nie naruszają istoty podstawowych praw i wolności oraz nie wykraczają poza to, co jest niezbędne i proporcjonalne w społeczeństwie demokratycznym, nie pozostają w sprzeczności z niniejszą Polityką.

Przy ocenie przepisów prawa i praktyk państw trzecich, które mogą wpływać na przestrzeganie zobowiązań wynikających z niniejszej Polityki, Członkowie Grupy powinni w szczególności należycie uwzględnić następujące elementy:

(i) konkretne okoliczności przekazania lub grupy przekazań oraz wszelkich planowanych dalszych przekazań w tym samym państwie trzecim lub do innego państwa trzeciego, w tym:

- o cele, w jakich dane są przekazywane i przetwarzane (*np.* marketing, HR, przechowywanie danych, wsparcie IT);
- o rodzaje podmiotów uczestniczących w przetwarzaniu (Podmiot Importujący oraz każdy dalszy odbiorca w ramach dalszego przekazywania danych);
- o sektor gospodarki, w którym dochodzi do przekazania lub grupy przekazań;
- o kategorie i format przekazywanych danych osobowych;
- o miejsce przetwarzania, w tym przechowywania danych; oraz
- o wykorzystywane kanały przekazywania danych;

(ii) przepisy prawa i praktyki obowiązujące w docelowych państwach trzecich, istotne z punktu widzenia okoliczności danego przekazania. Mogą one obejmować: (a) przepisy wymagające ujawnienia danych organom publicznym lub zezwalające takim organom na dostęp do danych; (b) przepisy przewidujące dostęp do tych danych podczas przekazywania danych pomiędzy państwami, w których znajdują się Podmioty Eksportujące, a państwami, w których znajdują się Podmioty Importujące; oraz (c) obowiązujące ograniczenia i zabezpieczenia.

(iii) Wszelkie odpowiednie umowne, techniczne lub organizacyjne zabezpieczenia wdrożone w celu uzupełnienia zabezpieczeń przewidzianych w niniejszej Polityce. Obejmuje to środki stosowane podczas przekazywania danych oraz w odniesieniu do przetwarzania danych osobowych w państwach docelowych.

Jeżeli konieczne jest wdrożenie dodatkowych zabezpieczeń, wykraczających poza środki przewidziane w niniejszej Polityce, Odpowiedzialny Członek BCR oraz właściwy Inspektor Ochrony Danych (IOD) lub Champion, stosownie do okoliczności, powinni zostać poinformowani oraz włączeni do procesu oceny. Członkowie Grupy mają obowiązek odpowiednio udokumentować taką ocenę, a także wybrane i wdrożone środki uzupełniające. Dokumentacja ta będzie udostępniana właściwemu organowi nadzorczemu na jego żądanie.

Podmioty Importujące niezwłocznie powiadomią Podmioty Eksportujące, jeżeli podczas stosowania niniejszej Polityki jako podstawy przekazywania danych oraz przez cały okres obowiązywania członkostwa mają podstawy sądzić, że podlegają lub zaczęły podlegać przepisom prawa bądź praktykom, które uniemożliwiałyby im wywiązanie się z obowiązków wynikających z niniejszej Polityki. Obejmuje to również niemożność wywiązania się z tych obowiązków w następstwie zmiany przepisów prawa obowiązujących w danym państwie trzecim lub zastosowania określonego środka (takiego jak żądanie ujawnienia danych osobowych). Informację tę należy również przekazać Odpowiedzialnemu Członkowi BCR.

Po zweryfikowaniu takiego powiadomienia właściwy Podmiot Eksportujący, wspólnie z Odpowiedzialnym Członkiem BCR oraz właściwym Inspektorem Ochrony Danych (IOD) lub Championem, stosownie do okoliczności, zobowiązuje się do niezwłocznego określenia dodatkowych środków (*np.* środków technicznych lub organizacyjnych zapewniających bezpieczeństwo i poufność), które mają zostać wdrożone przez Podmiot

Eksportujący i/lub Podmiot Importujący, tak aby umożliwić im wywiązanie się z obowiązków wynikających z niniejszej Polityki. To samo ma zastosowanie, jeżeli Podmiot Eksportujący ma uzasadnione podstawy, by sądzić, że Podmiot Importujący nie jest już w stanie wywiązywać się ze swoich obowiązków wynikających z niniejszej Polityki.

W przypadku gdy właściwy Podmiot Eksportujący, wspólnie z Odpowiedzialnym Członkiem BCR oraz właściwym Inspektorem Ochrony Danych (IOD) lub Championem, stosownie do okoliczności, ocenią, że nie jest możliwe zapewnienie zgodności z niniejszą Polityką w odniesieniu do danego przekazania lub grupy przekazań, nawet przy zastosowaniu środków uzupełniających, albo gdy tak nakaże właściwy organ nadzorczy, właściwy Podmiot Eksportujący zobowiązuje się zawiesić dane przekazanie lub grupę przekazań, a także wszystkie inne przekazania, w przypadku których ta sama ocena i jej uzasadnienie prowadziłyby do analogicznego wniosku, do czasu ponownego zapewnienia zgodności albo zakończenia przekazywania danych.

Po takim zawieszeniu Podmiot Eksportujący musi zakończyć przekazanie lub grupę przekazań, jeżeli nie można zapewnić zgodności z niniejszą Polityką i zgodność nie zostanie przywrócona w ciągu jednego miesiąca od dnia zawieszenia. W takim przypadku dane osobowe przekazane przed zawieszeniem oraz wszelkie ich kopie powinny, zgodnie z wyborem Podmiotu Eksportującego, zostać w całości zwrócone lub zniszczone.

Odpowiedzialny Członek BCR oraz właściwy Inspektor Ochrony Danych (IOD) lub Champion, stosownie do okoliczności, poinformują wszystkich pozostałych Członków Grupy o przeprowadzonej ocenie i jej wynikach, tak aby zidentyfikowane środki uzupełniające były stosowane w przypadku realizowania tego samego rodzaju przekazań przez innych Członków Grupy lub, jeżeli nie będzie możliwe wdrożenie skutecznych środków uzupełniających, aby takie przekazania zostały zawieszone lub zakończone.

Podmioty Eksportujące są również zobowiązane do bieżącego monitorowania, a w stosownych przypadkach także, we współpracy z Podmiotami Importującymi, zmian zachodzących w państwach trzecich, do których przekazano dane osobowe, jeżeli zmiany te mogą wpływać na pierwotną ocenę poziomu ochrony oraz decyzje podjęte w odniesieniu do takich przekazań.

Zasada 13B - Podmioty Importujące zapewnią, że w przypadku otrzymania prawnie wiążącego żądania organu władzy publicznej, wydanego na podstawie prawa kraju docelowego i dotyczącego ujawnienia danych osobowych przekazanych zgodnie z niniejszą Polityką, lub w razie powzięcia informacji o bezpośrednim dostępie organów władzy publicznej do danych osobowych przekazanych zgodnie z niniejszą Polityką na podstawie prawa kraju docelowego, niezwłocznie powiadomią o tym Podmiot Eksportujący oraz, w miarę możliwości, osobę, której dane dotyczą (w razie potrzeby przy wsparciu Podmiotu Eksportującego).

Podmioty Importujące niezwłocznie powiadomią właściwy Podmiot Eksportujący oraz, w miarę możliwości, osobę, której dane dotyczą (w razie potrzeby przy wsparciu Podmiotu Eksportującego), jeżeli:

- otrzymają prawnie wiążące żądanie organu władzy publicznej, wydane na podstawie prawa kraju docelowego lub innego państwa trzeciego, dotyczące ujawnienia danych osobowych przekazanych zgodnie z niniejszą Polityką (powiadomienie powinno zawierać informacje o żądanych danych osobowych, organie występującym z żądaniem, podstawie prawnej żądania oraz udzielonej odpowiedzi); lub

- powezmą informację o bezpośrednim dostępie organów władzy publicznej do danych osobowych przekazanych zgodnie z niniejszą Polityką zgodnie z prawem kraju docelowego (powiadomienie powinno zawierać wszystkie informacje dostępne Podmiotowi Importującemu).

Jeżeli Podmiot Importujący będzie objęty zakazem powiadomienia Podmiotu Eksportującego lub osoby, której dane dotyczą, o takim dostępie, dołoży wszelkich starań w celu uzyskania uchylenia tego zakazu, aby móc przekazać Podmiotowi Eksportującemu możliwie jak najwięcej informacji w możliwie najkrótszym terminie, oraz udokumentuje podjęte działania, tak aby móc je wykazać na żądanie Podmiotu Eksportującego.

Podmiot Importujący będzie w regularnych odstępach czasu przekazywał Podmiotowi Eksportującemu możliwie jak najwięcej istotnych informacji dotyczących otrzymanych żądań, w szczególności liczby żądań, rodzaju żądanych danych, organu lub organów występujących z żądaniem, informacji o tym, czy żądania zostały zakwestionowane, oraz wyników tych działań. Jeżeli Podmiot Importujący jest lub zostanie objęty częściowym albo całkowitym zakazem przekazywania Podmiotowi Eksportującemu powyższych informacji, bez zbędnej zwłoki poinformuje o tym Podmiot Eksportujący.

Podmiot Importujący będzie przechowywał wyżej wymienione informacje tak długo, jak długo dane podlegają zabezpieczeniom przewidzianym w niniejszej Polityce, oraz będzie udostępniał je właściwemu organowi nadzorczemu na jego żądanie.

Podmiot Importujący oceni zgodność z prawem żądania ujawnienia danych, w szczególności to, czy mieści się ono w granicach uprawnień przyznanych organowi władzy publicznej występującemu z żądaniem, oraz zakwestionuje to żądanie, jeżeli po wnikliwej analizie uzna, że istnieją uzasadnione podstawy, aby przyjąć, iż jest ono niezgodne z przepisami prawa kraju docelowego, właściwymi zobowiązaniami wynikającymi z prawa międzynarodowego oraz zasadami kurtuazji międzynarodowej. Na tych samych warunkach Podmiot Importujący będzie korzystał z dostępnych środków odwoławczych. W razie zakwestionowania żądania Podmiot Importujący wystąpi o zastosowanie środków tymczasowych w celu zawieszenia skutków tego żądania do czasu rozstrzygnięcia sprawy co do istoty przez właściwy sąd. Podmiot Importujący nie ujawni żądanych danych osobowych do czasu, aż będzie do tego zobowiązany na podstawie właściwych przepisów proceduralnych.

Podmiot Importujący udokumentuje swoją ocenę prawną oraz wszelkie działania podjęte w celu zakwestionowania żądania ujawnienia danych, a także, w zakresie dozwolonym przez przepisy prawa kraju docelowego, udostępni tę dokumentację Podmiotowi Eksportującemu. Dokumentacja ta będzie również udostępniana właściwemu organowi nadzorczemu na jego żądanie.

Odpowiadając na żądanie ujawnienia danych, Podmiot Importujący przekaże wyłącznie minimalny dopuszczalny zakres informacji, kierując się rozsądną interpretacją treści żądania.

W każdym przypadku Członkowie Grupy zapewnią, aby przekazywanie danych osobowych organom władzy publicznej na podstawie niniejszej Polityki nie miało charakteru masowego, nieproporcjonalnego ani nieukierunkowanego w sposób wykraczający poza to, co jest niezbędne w społeczeństwie demokratycznym.

ZASADA 14 - NIEPRZESTRZEGANIE POLITYKI I USTANIE JEJ OBOWIĄZYWANIA

Zasada 14A - Podmioty Eksportujące będą przekazywać dane osobowe wyłącznie Podmiotom Importującym, które przystąpiły do niniejszej Polityki i są w stanie zapewnić przestrzeganie jej postanowień.

Żadne przekazanie danych na podstawie niniejszej Polityki nie będzie dokonywane do Członka Grupy, chyba że taki Członek Grupy przystąpił do niniejszej Polityki i jest w stanie zapewnić przestrzeganie jej postanowień. Jeżeli Podmiot Importujący z jakiegokolwiek powodu nie jest w stanie przestrzegać niniejszej Polityki, ma obowiązek niezwłocznie poinformować o tym Podmiot Eksportujący. W przypadku gdy Podmiot Importujący narusza niniejszą Politykę lub nie jest w stanie jej przestrzegać, Podmiot Eksportujący zawiesi przekazanie albo odstąpi od jego dokonania.

Podmiot Importujący, zgodnie z wyborem Podmiotu Eksportującego, niezwłocznie zwróci lub usunie w całości przekazane dane osobowe, jeżeli:

- Podmiot Eksportujący zawiesił przekazywanie danych, a zgodność z niniejszą Polityką nie została przywrócona w rozsądnym terminie, nie później jednak niż w ciągu jednego miesiąca od dnia zawieszenia; lub
- Podmiot Importujący dopuścił się istotnego lub uporczywego naruszenia niniejszej Polityki; lub
- Podmiot Importujący nie zastosował się do wiążącego orzeczenia właściwego sądu lub decyzji właściwego organu nadzorczego dotyczących jego obowiązków wynikających z niniejszej Polityki.

To samo dotyczy wszelkich kopii danych. Podmiot Importujący potwierdzi Podmiotowi Eksportującemu usunięcie danych. Do czasu usunięcia lub zwrotu danych Podmiot Importujący nadal będzie zapewniał przestrzeganie niniejszej Polityki. Jeżeli przepisy prawa uniemożliwiają Podmiotowi Importującemu zwrot lub usunięcie przekazanych danych osobowych, Podmiot Importujący zapewnia, że nadal będzie przestrzegał niniejszej Polityki oraz będzie przetwarzał dane wyłącznie w zakresie i przez okres wymagane przepisami prawa.

Zasada 14B - Podmiot Importujący, który przestaje być związany niniejszą Polityką, zapewni odpowiednie przechowywanie, zwrot lub usunięcie danych osobowych, stosownie do okoliczności.

Podmiot Importujący, który przestaje być związany niniejszą Polityką, może stosownie do okoliczności zachować, zwrócić lub usunąć dane osobowe otrzymane na podstawie niniejszej Polityki. Jeżeli Podmiot Eksportujący i Podmiot Importujący uzgodnią, że dane mogą pozostać u Podmiotu Importującego, ochrona przewidziana w niniejszej Polityce musi zostać zachowana.

SEKCJA C: UPRAWNIENIA OSÓB TRZECICH BĘDĄCYCH BENEFICJENTAMI

C.1 Osoby, których dane osobowe są przekazywane do Podmiotu Importującego, muszą mieć możliwość korzystania z określonych praw jako osoby trzecie będące beneficjentami. W tym celu osoby, których dane dotyczą, mogą dochodzić przestrzegania postanowień:

- Zasady 1B i 1C Polityki (dotyczących rzetelności i zgodności z prawem oraz przetwarzania szczególnych kategorii danych osobowych);
- Zasady 2 Polityki (dotyczącej przejrzystości i przetwarzania danych osobowych wyłącznie w określonym celu);
- Zasady 3 Polityki (dotyczącej minimalizacji danych, ich prawidłowości oraz ograniczenia okresów przechowywania);
- Zasady 4 Polityki (dotyczącej odpowiednich środków bezpieczeństwa oraz obowiązków związanych ze zgłaszaniem naruszeń ochrony danych osobowych);
- Zasady 5 Polityki (dotyczącej poszanowania praw osób, których dane dotyczą);
- Zasady 6 Polityki (dotyczącej zapewnienia odpowiedniego poziomu ochrony przy przekazywaniu i dalszym przekazywaniu danych osobowych);
- Zasady 10 Polityki (dotyczącej rozpatrywania skarg);

- Zasady 11 Polityki (dotyczącej współpracy z właściwymi organami nadzorczymi);
- Zasady 12 Polityki (dotyczącej aktualizacji zasad);
- Zasady 13 Polityki (dotyczącej postępowania w przypadku, gdy prawo krajowe uniemożliwia przestrzeganie Polityki);
- postanowień zawartych w punktach C.1-C.3, przyznających osobom trzecim prawa beneficjenta oraz określających zasady odpowiedzialności i jurysdykcji wynikające z niniejszej Polityki; oraz
- prawa dostępu do Polityki dostępnej na stronie internetowej, w wewnętrznej sieci spółki (dostępnej dla pracowników) lub do uzyskania jej wersji papierowej, a także do listy Członków Grupy, którzy przystąpili do niniejszej Polityki.

Prawa te mogą być wykonywane poprzez:

- *wniesienie skargi* - osoby, których dane dotyczą, mogą złożyć skargę do Członka Grupy (zgodnie z Procedurą rozpatrywania skarg określoną w Załączniku 2) oraz do organu nadzorczego w państwie członkowskim, w którym doszło do domniemanego naruszenia, albo w którym osoba, której dane dotyczą, zwykle pracuje lub ma miejsce zwykłego pobytu; i/lub
- *wniesienie powództwa* - osoby, których dane dotyczą, mogą wnieść powództwo przeciwko Członkom Grupy przed sądami państwa członkowskiego, w którym dany Członek Grupy posiada jednostkę organizacyjną, lub przed sądami państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu.

Jak wyjaśniono w sekcjach C.2-C.4, w przypadku naruszenia popełnionego przez Członka Grupy mającego siedzibę poza EOG osoby, których dane dotyczą, zachowują prawo do wniesienia skargi oraz wytoczenia powództwa przeciwko wyznaczonemu Odpowiedzialnemu Członkowi BCR, tak jak gdyby naruszenie zostało popełnione przez ten podmiot w państwie członkowskim, w którym ma on siedzibę.

Prawa te nie obejmują tych elementów niniejszej Polityki, które dotyczą wewnętrznych mechanizmów wdrożonych przez Członków Grupy, takich jak szczegóły dotyczące szkoleń, programu audytów, sieci ds. zgodności oraz mechanizmu jej aktualizacji.

Ponadto Członkowie Grupy uznają, że osoby, których dane dotyczą, mogą być reprezentowane przez podmiot, organizację lub stowarzyszenie niedziałające dla zysku, na warunkach określonych w art. 80 ust. 1 RODO.

C.2 Osoby, których dane dotyczą, mogą również dochodzić odpowiednich środków ochrony prawnej od Odpowiedzialnego Członka BCR, który zobowiązuje się podjąć wszelkie niezbędne działania w celu usunięcia naruszeń postanowień wymienionych w sekcji C.1 przez Podmiot Importujący oraz, w stosownych przypadkach, dochodzić od Odpowiedzialnego Członka BCR odszkodowania za wszelką szkodę majątkową lub niemajątkową poniesioną w wyniku naruszenia postanowień wymienionych w sekcji C.1 przez Podmiot Importujący, zgodnie z orzeczeniem właściwego sądu lub innego właściwego organu.

C.3 Dla uniknięcia wątpliwości osobom, których dane dotyczą, przysługują prawa osób trzecich będących beneficjentami określone w niniejszej sekcji C, a właściwe sądy państw członkowskich oraz właściwe

organy nadzorcze zachowują właściwość, jak gdyby naruszenia postanowień opisanych w niniejszej sekcji C dopuścił się Odpowiedzialny Członek BCR.

C.4 W przypadku wniesienia powództwa dotyczącego szkody poniesionej przez osobę, której dane dotyczą, w wyniku naruszenia niniejszej Polityki, Członkowie Grupy uzgodnili, że ciężar wykazania, iż Podmiot Importujący nie ponosi odpowiedzialności za naruszenie lub że do naruszenia w ogóle nie doszło, spoczywa na Odpowiedzialnym Członku BCR.

CZĘŚĆ III: ZAŁĄCZNIKI

ZAŁĄCZNIK 1

PROGRAM AUDYTU

1. WPROWADZENIE

1.1 Członkowie Grupy są zobowiązani do przeprowadzania audytów zgodności z niniejszą Polityką oraz do spełniania określonych wymagań w tym zakresie. Niniejszy dokument opisuje sposób, w jaki Członkowie Grupy spełniają te wymagania.

1.2 Do *standardowej działalności operacyjnej* (BAU) Inspektorów Ochrony Danych (IOD) oraz Championów należy udzielanie wytycznych dotyczących przetwarzania danych osobowych objętego niniejszą Polityką oraz ocena przetwarzania danych osobowych prowadzonego przez Członków Grupy pod kątem potencjalnych ryzyk związanych z ochroną danych osobowych w ramach bieżącej działalności. Przetwarzanie danych osobowych podlega zatem szczegółowemu przeglądowi i bieżącej ocenie.

1.3 Jako globalna druga linia obrony (2LoD), Korporacyjne Biuro ds. Ochrony Danych odpowiada za monitorowanie i kontrolę, w tym za nadzór nad zgodnością Grupy Santander z przepisami o ochronie danych.

1.4 Z kolei Program Audytu obejmuje formalną, niezależną ocenę przeprowadzaną przez trzecią linię obrony (3LoD) w celu oceny zgodności z niniejszą Polityką, zgodnie z wymaganiami właściwych organów nadzorczych. Opinia wydana przez trzecią linię obrony (3LoD) ma charakter niezależny i nie zastępuje obowiązków pierwszej linii obrony (1LoD) i drugiej linii obrony (2LoD) w zakresie kontroli i nadzoru. Obszary te również będą objęte zakresem audytu podczas oceny stopnia wdrożenia i stosowania niniejszej Polityki.

2. PODEJŚCIE

2.1 <u>Przegląd procesu audytu</u>

Podmiot odpowiedzialny za przeprowadzanie audytów zgodności z niniejszą Polityką oraz za zapewnienie, że obejmują one wszystkie jej aspekty, może różnić się w zależności od specyfiki danego Członka Grupy. Zazwyczaj audyty są nadzorowane, stosownie do okoliczności, przez akredytowanych audytorów wewnętrznych lub zewnętrznych, którym zagwarantowano niezależność w wykonywaniu obowiązków związanych z tymi audytami. Właściwy audytor będzie odpowiedzialny za zapewnienie, że wszelkie problemy lub przypadki niezgodności zostaną zgłoszone najwyższemu kierownictwu oraz że wszelkie działania korygujące niezbędne do zapewnienia zgodności zostaną podjęte w rozsądnym terminie.

2.2 <u>Termin i zakres audytu</u>

2.2.1 Dział Audytu Wewnętrznego, zgodnie ze swoją metodyką oceny ryzyka, ustali harmonogram przeprowadzania audytów w ramach maksymalnego czteroletniego cyklu audytowego.

Niemniej jednak pierwsze audyty zostaną przeprowadzone w ciągu pierwszych 24 miesięcy od formalnego zatwierdzenia niniejszej Polityki i uzyskania przez nią mocy obowiązującej. Kolejne audyty będą przeprowadzane zgodnie z obowiązującą metodyką audytu opartą na analizie ryzyka, zgodnie z opisem zawartym w pierwszym akapicie sekcji 2.2.

We wszystkich przypadkach Członkowie Grupy będą zobowiązani do przeprowadzenia audytu, jeżeli: (i) istnieją przesłanki wskazujące na nieprzestrzeganie niniejszej Polityki; lub (ii) Zespół ds. Prywatności zażąda przeprowadzenia audytu doraźnego (ad hoc).

2.2.2 Podobnie zakres i zasięg audytu zostaną określone przez Dział Audytu Wewnętrznego na podstawie analizy ryzyka przeprowadzonej zgodnie z zatwierdzoną metodyką.

2.2.3 Wszystkie aspekty niniejszej Polityki (*np.* aplikacje, systemy IT, dalsze przekazywanie danych itp.), w tym metody oraz plany działań zapewniające wdrożenie działań korygujących, będą poddawane przeglądowi zgodnie z podejściem opartym na analizie ryzyka w celu określenia szczegółowego zakresu audytu. Przeglądy będą przeprowadzane, zgodnie z powyższym opisem, w odpowiednich regularnych odstępach czasu.

2.3 Audytorzy

2.3.1 Audyty przewidziane w niniejszym dokumencie będą przeprowadzane przez audytorów wewnętrznych z Działu Audytu Wewnętrznego lub, stosownie do okoliczności, przez akredytowanych audytorów zewnętrznych. W przypadku gdy audyty są przeprowadzane przez audytorów zewnętrznych, muszą zostać spełnione następujące warunki:

(a) przed ich wyborem należy przeprowadzić odpowiednią procedurę należytej staranności, aby upewnić się, że posiadają oni odpowiednie kwalifikacje i status umożliwiające realizację tego zadania; oraz

(b) należy zawrzeć z nimi umowę regulującą świadczenie usług zgodnie z obowiązującymi przepisami.

2.4 Niezależność

2.4.1 Osoby odpowiedzialne za ustalanie programu audytu lub przeprowadzanie audytów mają zagwarantowaną niezależność w wykonywaniu swoich obowiązków.

2.5 Raport

2.5.1 Po zakończeniu audytu, w zależności od jego charakteru, raport oraz ustalenia zostaną udostępnione najwyższemu kierownictwu, Korporacyjnemu Biuru ds. Ochrony Danych, właściwemu Inspektorowi Ochrony Danych (IOD) lub Championowi, a także przekazane Komitetowi Audytu Rady oraz Radzie Odpowiedzialnego Członka BCR. Raport z audytu będzie również zawierał informacje o wymaganych działaniach korygujących, zalecenia oraz terminy ich realizacji.

2.5.2 Członkowie Grupy uzgodnili, że na żądanie właściwego organu nadzorczego udostępnią kopie wyników każdego audytu niniejszej Polityki.

2.5.3 Właściwy Inspektor Ochrony Danych (IOD) lub Champion będzie odpowiedzialny za utrzymywanie kontaktów z właściwymi organami nadzorczymi w celu przekazania wskazanych powyżej informacji.

ZAŁĄCZNIK 2

PROCEDURA ROZPATRYWANIA SKARG

1. WPROWADZENIE

1.1 Celem niniejszej Procedury rozpatrywania skarg jest wyjaśnienie, w jaki sposób będą rozpatrywane skargi wnoszone przez osoby, których dane osobowe są przetwarzane przez Członków Grupy zgodnie z niniejszą Polityką.

2. JAK OSOBY, KTÓRYCH DANE DOTYCZĄ, MOGĄ SKŁADAĆ SKARGI

Wszystkie skargi osób, których dane osobowe są przetwarzane zgodnie z niniejszą Polityką, mogą być składane na piśmie (w tym pocztą elektroniczną) do właściwego Inspektora Ochrony Danych (IOD) lub Championa, stosownie do okoliczności. Osoby, których dane dotyczą, mogą złożyć skargę, korzystając z następujących danych kontaktowych:

Adresat: Zespół ds. Prywatności

Adres: [Wpisać adres pocztowy]

E-mail: Lista odpowiednich adresów e-mail jest dostępna tutaj.

W każdym przypadku, jeżeli skarga zostanie wniesiona w inny sposób, również zostanie rozpatrzona, pod warunkiem że właściwy Członek Grupy zostanie o niej odpowiednio poinformowany.

3. KTO ROZPATRUJE SKARGI?

3.1 Właściwy Inspektor Ochrony Danych (IOD) lub Champion, stosownie do okoliczności, będzie rozpatrywał wszystkie skargi dotyczące przetwarzania danych osobowych na podstawie niniejszej Polityki. Inspektor Ochrony Danych (IOD) lub Champion, stosownie do okoliczności, będzie współpracował z właściwymi jednostkami biznesowymi w celu zbadania skargi oraz skoordynuje przygotowanie odpowiedzi, obejmującej informacje o działaniach podjętych w związku ze skargą, które zostaną przekazane skarżącemu.

3.2 Jaki jest termin udzielenia odpowiedzi?

IOD lub Champion, przy wsparciu Zespołu ds. Prywatności, potwierdzi otrzymanie skargi zainteresowanej osobie, której dane dotyczą, w terminie dziesięciu dni roboczych, a następnie przeprowadzi postępowanie wyjaśniające i udzieli merytorycznej odpowiedzi, przekazując informacje o podjętych działaniach bez zbędnej zwłoki, nie później jednak niż w ciągu jednego miesiąca kalendarzowego. Jeżeli ze względu na złożoność skargi lub liczbę wniosków udzielenie merytorycznej odpowiedzi w tym terminie nie będzie możliwe, Inspektor Ochrony Danych (IOD) lub Champion, przy wsparciu Zespołu ds. Prywatności, poinformuje skarżącego o przyczynach opóźnienia w ciągu jednego miesiąca kalendarzowego od otrzymania skargi oraz wskaże szacowany termin udzielenia odpowiedzi, nie dłuższy niż kolejne dwa miesiące kalendarzowe od dnia powiadomienia osoby, której dane dotyczą, o przedłużeniu tego terminu.

Jeżeli termin udzielenia odpowiedzi nie zostanie dotrzymany, a odpowiedź na skargę ulegnie opóźnieniu bez uprzedniego poinformowania o przyczynach, osoba, której dane dotyczą, może poinformować o tym Inspektora Ochrony Danych (IOD) lub Championa. Inspektor Ochrony Danych

(IOD) lub Champion bez zbędnej zwłoki, nie później jednak niż w terminie dziesięciu dni kalendarzowych, wyjaśni przyczyny opóźnienia oraz poinformuje osobę, której dane dotyczą, o działaniach podjętych do tego czasu. Sprawa zostanie przekazana do Korporacyjnego Biura ds. Ochrony Danych wraz z raportem zawierającym uzasadnienie i określającym działania, jakie należy podjąć. Korporacyjne Biuro ds. Ochrony Danych przeanalizuje sprawę i doradzi Inspektorowi Ochrony Danych (IOD) lub Championowi, w jaki sposób jak najszybciej rozwiązać kwestie będące przedmiotem skargi. W każdym przypadku osoba, której dane dotyczą, może również skorzystać z praw opisanych w sekcji 3.4 niniejszego Załącznika 2.

3.3 Jeżeli skarżący kwestionuje ustalenia lub odmowę rozpatrzenia skargi

Jeżeli skarga zostanie uznana za uzasadnioną, IOD lub Champion podejmie niezbędne działania w celu rozwiązania problemu zgłoszonego przez osobę, której dane dotyczą, i odpowiednio poinformuje ją o podjętych działaniach.

Jeżeli skarżący kwestionuje odpowiedź Inspektora Ochrony Danych (IOD) lub Championa (w tym odmowę rozpatrzenia skargi lub uwzględnienia zawartych w niej żądań) albo jakikolwiek element ustaleń, może poinformować o tym właściwego Inspektora Ochrony Danych (IOD) lub Championa. Sprawa zostanie przekazana do Korporacyjnego Biura ds. Ochrony Danych, które przeanalizuje sprawę i za pośrednictwem IOD lub Championa danej jednostki poinformuje skarżącego o ostatecznej decyzji, polegającej na utrzymaniu pierwotnych ustaleń albo zastąpieniu ich nowymi. Korporacyjne Biuro ds. Ochrony Danych odpowie skarżącemu w terminie jednego miesiąca kalendarzowego od dnia przekazania sprawy. Jeżeli ze względu na złożoność skargi udzielenie merytorycznej odpowiedzi w tym terminie nie będzie możliwe, Korporacyjne Biuro ds. Ochrony Danych poinformuje skarżącego o przyczynach opóźnienia w terminie jednego miesiąca kalendarzowego od dnia otrzymania przekazanej sprawy oraz wskaże szacowany termin udzielenia odpowiedzi, nie dłuższy niż kolejne dwa miesiące kalendarzowe. Jeżeli skarga zostanie uznana za zasadną, Korporacyjne Biuro ds. Ochrony Danych zapewni podjęcie wszelkich niezbędnych działań będących następstwem tego rozstrzygnięcia.

3.4 Alternatywne sposoby składania skarg

Osobom, których dane osobowe są przetwarzane zgodnie z niniejszą Polityką, przysługuje również prawo do: (i) złożenia skargi do organu nadzorczego w państwie członkowskim, w którym doszło do domniemanego naruszenia, albo w którym osoba, której dane dotyczą, zwykle pracuje lub ma miejsce zwykłego pobytu; i/lub (ii) wniesienia powództwa do właściwego sądu państwa członkowskiego, w którym Członek Grupy ma siedzibę, lub państwa, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu. Jak wyjaśniono w sekcjach C.2-C.4, w przypadku naruszenia popełnionego przez Członka Grupy mającego siedzibę poza EOG osoby, których dane dotyczą, zachowują prawo do wniesienia skargi oraz wytoczenia powództwa przeciwko wyznaczonemu Odpowiedzialnemu Członkowi BCR, tak jak gdyby naruszenie zostało popełnione przez ten podmiot w państwie członkowskim, w którym ma on siedzibę. Prawa te przysługują niezależnie od tego, czy osoba, której dane dotyczą, wcześniej złożyła skargę do Członka Grupy zgodnie z niniejszą Procedurą rozpatrywania skarg.

ZAŁĄCZNIK 3

PROCEDURA WSPÓŁPRACY

1. PROCEDURA WSPÓŁPRACY

1.1 Niniejsza Procedura współpracy określa sposób, w jaki Członkowie Grupy będą współpracować z właściwymi organami nadzorczymi, poddawać się prowadzonym przez nie audytom i kontrolom (w tym, w razie potrzeby, kontrolom na miejscu), a także uwzględniać ich zalecenia oraz stosować się do ich decyzji we wszystkich kwestiach związanych z niniejszą Polityką.

1.2 W razie potrzeby Członkowie Grupy zapewnią odpowiedni personel do prowadzenia dialogu z właściwym organem nadzorczym w sprawach dotyczących niniejszej Polityki.

1.3 Na żądanie właściwy Inspektor Ochrony Danych (IOD), Champion lub Dział Audytu Wewnętrznego, stosownie do okoliczności, przekaże właściwemu organowi nadzorczemu kopie wyników audytów przeprowadzonych zgodnie z Załącznikiem 1 oraz wszelkie informacje dotyczące operacji przetwarzania objętych niniejszą Polityką. Organowi zostanie jednocześnie przypomniany obowiązek zachowania tajemnicy zawodowej.

1.4 Członkowie Grupy zgadzają się, że właściwe organy nadzorcze mogą przeprowadzać audyty ochrony danych osobowych lub kontrole (w tym, w razie potrzeby, na miejscu) zgodnie z europejskim prawem ochrony danych właściwego Podmiotu Eksportującego.

1.5 Wszyscy Członkowie Grupy wyrażają zgodę na poddawanie się audytom prowadzonym przez właściwe organy nadzorcze zgodnie z obowiązującymi u tych organów procedurami audytowymi.

1.6 Członkowie Grupy zgadzają się, że wszelkie spory związane z wykonywaniem przez właściwy organ nadzorczy jego uprawnień nadzorczych w odniesieniu do niniejszej Polityki będą rozstrzygane przez sądy państwa członkowskiego, w którym organ ten ma siedzibę, zgodnie z jego prawem procesowym.

ZAŁĄCZNIK 4

PROCEDURA AKTUALIZACJI

1. WPROWADZENIE I ZASADY OGÓLNE

1.1 Niniejsza Procedura aktualizacji określa sposób przekazywania informacji o zmianach w niniejszej Polityce właściwym organom nadzorczym, osobom, których dane dotyczą, oraz Członkom Grupy, którzy przystąpili do niniejszej Polityki.

1.2 Niniejsza Polityka będzie na bieżąco aktualizowana, aby odzwierciedlać aktualny stan w zakresie ochrony danych osobowych.

2. ISTOTNE ZMIANY W POLITYCE

2.1 Inspektor Ochrony Danych Banco Santander oraz Korporacyjny Dział Prawny będą z wyprzedzeniem informować Hiszpańską Agencję Ochrony Danych („**BCR Lead**") o wszelkich istotnych zmianach w Polityce (*tj.* wszelkich zmianach, które mogłyby obniżyć poziom ochrony zapewniany przez Politykę lub w istotny sposób wpływać na jej postanowienia, *np.* dotyczących jej wiążącego charakteru) a za pośrednictwem BCR Lead także także pozostałe właściwe organy nadzorcze. Takie powiadomienie będzie zawierało krótkie wyjaśnienie przyczyn aktualizacji. Właściwy organ nadzorczy oceni również, czy wprowadzone zmiany wymagają ponownego zatwierdzenia.

3. INNE ZMIANY W POLITYCE

3.1 Inspektor Ochrony Danych Banco Santander oraz Korporacyjny Dział Prawny będą, na żądanie oraz co najmniej raz w roku, przekazywać BCR Lead (a za jego pośrednictwem pozostałym właściwym organom nadzorczym) informacje o zmianach w Polityce lub o ich braku. Coroczna aktualizacja będzie również obejmować ponowne potwierdzenie, że Odpowiedzialny Członek BCR dysponuje wystarczającymi aktywami lub poczynił odpowiednie ustalenia umożliwiające wypłatę odszkodowania za szkody wynikające z naruszenia niniejszej Polityki.

3.2 Przykłady takich zmian obejmują zmiany o charakterze administracyjnym (w tym aktualizację listy Członków Grupy), zmiany wynikające ze zmian europejskiego prawa ochrony danych lub z aktów prawnych, orzeczeń sądowych oraz środków i wytycznych organów nadzorczych, w tym wytycznych Europejskiej Rady Ochrony Danych. Banco Santander przekaże również BCR Lead oraz pozostałym właściwym organom nadzorczym krótkie wyjaśnienie przyczyn każdej zgłoszonej zmiany Polityki.

4. NOWI CZŁONKOWIE GRUPY

4.1 Inspektorzy Ochrony Danych (IOD) i Championowie, przy wsparciu Zespołu ds. Prywatności, zapewnią, że wszyscy nowi Członkowie Grupy przystąpili do niniejszej Polityki oraz są w stanie zapewnić przestrzeganie jej postanowień przed dokonaniem przekazania im danych osobowych.

5. KOMUNIKOWANIE I REJESTROWANIE ZMIAN W POLITYCE

5.1 Polityka zawiera rejestr zmian określający daty kolejnych wersji oraz szczegóły wszystkich wprowadzonych zmian. Korporacyjny Dział Prawny będzie prowadził aktualny wykaz zmian w Polityce, a Korporacyjne Biuro ds. Ochrony Danych będzie prowadziło listę Członków Grupy, którzy przystąpili do niniejszej Polityki.

5.2 Korporacyjny Dział Prawny, przy wsparciu Korporacyjnego Biura ds. Ochrony Danych, będzie informował o wszystkich zmianach w Polityce, zarówno istotnych, jak i pozostałych:

(a) Członków Grupy, którzy przystąpili do niniejszej Polityki, bez zbędnej zwłoki, oraz opublikuje zaktualizowaną wersję Polityki w wewnętrznej sieci Grupy Santander;

(b) osoby, których dane dotyczą, objęte niniejszą Polityką, regularnie, za pośrednictwem strony internetowej spółki (Web Corporativa Santander); oraz

(c) na żądanie, za pośrednictwem właściwych lokalnych Inspektorów Ochrony Danych (IOD) (lub osób pełniących równoważną funkcję), właściwe organy nadzorcze.