SANTANDER GROEP

BELEID INZAKE BINDENDE BEDRIJFSVOORSCHRIFTEN VOOR VERWERKINGSVERANTWOORDELIJKEN

INHOUDSOPGAVE PAGINA

INLEIDING 3

DEEL I: ACHTERGROND EN MAATREGELEN 6

REGEL 1 – RECHTMATIGHEID EN EERLIJKHEID 15

REGEL 2 – HET WAARBORGEN VAN TRANSPARANTIE EN HET UITSLUITEND VERWERKEN VAN PERSOONSGEGEVENS VOOR EEN BEKEND DOEL 17

REGEL 3 – HET WAARBORGEN VAN DE GEGEVENSKWALITEIT 19

REGEL 4 – HET TREFFEN VAN PASSENDE BEVEILIGINGSMAATREGELEN 20

REGEL 5 – EERBIEDIGING VAN DE RECHTEN VAN BETROKKENEN 22

REGEL 6 – HET WAARBORGEN VAN ADEQUATE BESCHERMING BIJ DOORGIFTE EN VERDERE DOORGIFTE 23

REGEL 7 – NALEVING EN VERANTWOORDING 24

REGEL 8 – TRAINING 27

REGEL 9 – AUDIT 28

REGEL 10 – KLACHTENAFHANDELING 28

REGEL 11 – SAMENWERKING MET TOEZICHTHOUDENDE AUTORITEITEN 28

REGEL 12 – ACTUALISERING VAN DE REGELS 28

REGEL 13 – MAATREGELEN INDIEN DE NATIONALE WETGEVING DE NALEVING VAN HET BELEID VERHINDERT 28

REGEL 14 – NIET-NALEVING VAN HET BELEID EN BEËINDIGING 32

DEEL III: BIJLAGEN 35

INLEIDING

Dit Beleid inzake bindende bedrijfsvoorschriften voor verwerkingsverantwoordelijken en de bijlagen daarbij (gezamenlijk het "**Beleid**") beschrijven de aanpak die Banco Santander, S.A. ("**Banco Santander**") hanteert met betrekking tot de bescherming en het beheer van persoonsgegevens door de leden van de Santander Groep – zoals hieronder gedefinieerd – die aan dit Beleid zijn gebonden, in het kader van de internationale doorgiften van genoemde persoonsgegevens tussen Groepsleden, zoals hieronder gedefinieerd.

Banco Santander is de moedermaatschappij en het hoofdkantoor van een van de grootste financiële groepen in Spanje, bestaande uit zowel Spaanse als buitenlandse dochterondernemingen ("**Santander Groep**"), die zich wereldwijd toeleggen op het verlenen van financiële diensten, voornamelijk op de volgende gebieden: (i) **Particulier en zakelijk bankieren**: omvat alle activiteiten van Santander op het gebied van particulier en zakelijk bankieren; (ii) **Corporate and Investment Banking**: ondersteunt zakelijke en institutionele klanten met diensten op maat en wholesale-producten met toegevoegde waarde via de divisies Markets, Investment Banking (Global Debt Finance en Corporate Finance) en Global Transactional Banking; (iii) **Vermogensbeheer en verzekeringen:** brengt private banking, vermogensbeheer en verzekeringen samen via Santander Private Banking, Santander Asset Management en Santander Insurance; (iv) **Digital Consumer Bank**: brengt het digitale Openbank-platform en Santander Consumer Finance samen, waardoor één uniform model ontstaat voor consumenten en autofinanciering in alle markten; en (v) **PagoNxt en Cards**: omvat PagoNxt, waar alle betalingsactiviteiten van Santander onder vallen, en Global Cards, de kaartactiviteiten en het platform van Santander, dat digitale betaalopties en wereldwijde technologische oplossingen biedt voor de banken van Santander en nieuwe klanten. Daarnaast bestaat de Santander Groep ook uit het **Corporate Centre en andere afdelingen die de hele Groep ondersteunen**: dit zijn de afdelingen die alle Groepsleden ondersteunen en helpen bij alle noodzakelijke zaken op groepsniveau die niet direct verband houden met hun kernactiviteit (bijv. personeelsbeheer, naleving van wettelijke verplichtingen, audits, risicobeheer enz.).

Naast andere definities die in dit Beleid zijn opgenomen, zijn de volgende termen van toepassing:

"**Toepasselijke lokale wetgeving inzake gegevensbescherming**" betekent elke nationale/lokale wet inzake gegevensbescherming (inclusief, indien van toepassing, de Europese wetgeving inzake gegevensbescherming) die van toepassing is op Groepsleden, zolang deze wetgeving de essentie van de fundamentele rechten en vrijheden respecteert en niet verder gaat dan wat in een democratische samenleving noodzakelijk en evenredig is, in overeenstemming met de vereisten van Regel 13 van dit Beleid;

"**bevoegde toezichthoudende autoriteit**" betekent de voor de Exporterende entiteit bevoegde toezichthoudende autoriteit in de EER;

"**verwerkingsverantwoordelijke**" betekent de natuurlijke of rechtspersoon, overheidsinstantie, dienst of ander orgaan die/dat, alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt;

"**Europa**" of "**EER**" verwijst naar de landen in de Europese Economische Ruimte;

"**Europese wetgeving inzake gegevensbescherming**" betekent de AVG en elke gegevensbeschermingswet van een EU-lidstaat, met inbegrip van lokale wetgeving ter uitvoering van de vereisten van de AVG, zoals secundaire wetgeving, in elk geval zoals van tijd tot tijd gewijzigd;

"**Exporterende entiteit**" betekent een Groepslid dat in Europa is gevestigd of anderszins onderworpen is aan de Europese wetgeving inzake gegevensbescherming en dat krachtens dit Beleid persoonsgegevens doorgeeft of anderszins beschikbaar stelt aan een Importerende entiteit;

"**AVG**" betekent Verordening (EU) 2016/679 (de Algemene Verordening Gegevensbescherming);

"**Groepslid**" betekent de leden van de Santander Groep die zich aan dit Beleid houden;

"**Importerende entiteit**" betekent een Groepslid dat buiten Europa is gevestigd en persoonsgegevens van een Exporterende entiteit ontvangt en de doorgegeven persoonsgegevens buiten de EER verwerkt;

"**Aansprakelijk BCR-lid**" betekent Banco Santander, (d.w.z. Banco Santander S.A. zoals hierboven gedefinieerd);

"**persoonsgegevens**" betekent alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Een identificeerbare natuurlijke persoon is iemand die direct of indirect kan worden geïdentificeerd, met name aan de hand van een ID zoals een naam, een identificatienummer, locatiegegevens, een online ID of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

"**verwerking**" betekent elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of reeksen van persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde middelen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, aanpassen of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, het samenvoegen of combineren, beperken, wissen of vernietigen;

"**verwerker**" verwijst naar een natuurlijke of rechtspersoon, overheidsinstantie, dienst of ander orgaan die/dat persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke;

"**profilering**" betekent elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij persoonlijke aspecten met betrekking tot een natuurlijke persoon worden geëvalueerd, met name om aspecten te analyseren of te voorspellen die betrekking hebben op de werkprestaties, de economische situatie, de gezondheid, de persoonlijke voorkeuren of interesses, de betrouwbaarheid of het gedrag, de locatie of de verplaatsingen van die natuurlijke persoon;

"**bijzondere categorieën persoonsgegevens**" of "**gevoelige gegevens**" betekent persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens of biometrische gegevens blijken die worden verwerkt met het oog op de unieke identificatie van een natuurlijke persoon, gegevens betreffende de gezondheid of gegevens betreffende het seksleven of de seksuele geaardheid van een natuurlijke persoon; en

"**toezichthoudende autoriteit**" betekent een onafhankelijke overheidsinstantie, die door een lidstaat in een Europees rechtsgebied is opgericht en die verantwoordelijk is voor het toezicht op de toepassing van de Europese wetgeving inzake gegevensbescherming, teneinde de grondrechten en vrijheden van natuurlijke personen met betrekking tot de verwerking te beschermen en het vrije verkeer van persoonsgegevens binnen de EER te faciliteren.

Dit Beleid is van toepassing op alle persoonsgegevens die onder de Europese wetgeving inzake gegevensbescherming vallen en die vervolgens worden doorgegeven door Exporterende entiteiten aan

Importerende entiteiten, alsmede op verdere doorgiften door Importerende entiteiten aan andere Importerende entiteiten of aan derden buiten de EER (overeenkomstig de vereisten van Regel 6 hieronder). Derhalve zijn alle verplichtingen en vereisten die krachtens dit Beleid aan Groepsleden worden opgelegd, van toepassing voor zover zij betrekking hebben op persoonsgegevens die onder die reikwijdte vallen.

Dit Beleid is van toepassing op alle dergelijke persoonsgegevens die door Groepsleden worden verwerkt, zoals beschreven in de secties "*Welke persoonsgegevens vallen onder dit Beleid?*" en "*Voor welke doeleinden worden persoonsgegevens krachtens dit Beleid doorgegeven?*".

Groepsleden en hun werknemers dienen dit Beleid bij de verwerking van persoonsgegevens in het kader hiervan volledig na te leven en te respecteren..

Dit Beleid vormt een aanvulling op, en vervangt of overschrijft geen specifieke vereisten of regels inzake vertrouwelijkheid of geheimhouding die van toepassing kunnen zijn op een bedrijfsonderdeel of afdeling binnen de Santander Groep of die worden vereist door de toepasselijke wetgeving (voor zover die wetgeving voldoet aan de vereisten van Regel 13 hieronder).

Dit Beleid, samen met een lijst van de huidige Groepsleden en hun contactgegevens zoals opgenomen in Bijlage 5, is gepubliceerd op de openbaar toegankelijke website van het bedrijf. U vindt het Beleid hier.

Toepasselijkheid op doorgiften door Groepsleden die niet onder de Europese wetgeving inzake gegevensbescherming vallen

Indien een Groepslid dat niet onder de Europese wetgeving inzake gegevensbescherming valt, eveneens beperkingen kent ten aanzien van internationale doorgiften van persoonsgegevens op grond van de voor dat land geldende Toepasselijke lokale wetgeving inzake gegevensbescherming en de lokale autoriteiten van dergelijke landen dit Beleid (geheel of gedeeltelijk, zoals vereist krachtens de Toepasselijke lokale wetgeving inzake gegevensbescherming) erkennen als een geldig mechanisme voor het legitimeren van internationale doorgiften van persoonsgegevens, kan dit Beleid ook van toepassing zijn op de persoonsgegevens die vanuit dergelijke landen worden doorgegeven aan de Importerende entiteiten. Ter verduidelijking: dit laat de toepassing van de Toepasselijke lokale wetgeving inzake gegevensbescherming op het Groepslid buiten Europa onverlet.

In deze gevallen dienen de bovenstaande definities zo te worden uitgelegd dat het Groepslid dat persoonsgegevens overdraagt en niet onderworpen is aan de Europese wetgeving inzake gegevensbescherming, wordt beschouwd als de Exporterende entiteit. Dienovereenkomstig dient het Beleid *mutatis mutandis* te worden uitgelegd en toegepast (bijvoorbeeld: de Europese wetgeving inzake gegevensbescherming dient te worden opgevat als de toepasselijke lokale wetgeving inzake gegevensbescherming, de bevoegde toezichthoudende autoriteit als de bevoegde lokale autoriteit in het desbetreffende rechtsgebied of de Lidstaat als het betrokken land).

In dit geval treedt het Groepslid dat persoonsgegevens overdraagt die niet onder de Europese wetgeving inzake gegevensbescherming vallen, op als het Aansprakelijke BCR-lid met betrekking tot dergelijke internationale doorgifte(n) van gegevens.

DEEL I: ACHTERGROND EN MAATREGELEN

WAT IS DE EUROPESE WETGEVING INZAKE GEGEVENSBESCHERMING?

De Europese wetgeving inzake gegevensbescherming geeft mensen het recht om te bepalen hoe hun persoonsgegevens worden verwerkt. Krachtens de Europese wetgeving inzake gegevensbescherming wordt een organisatie die persoonsgegevens voor eigen doeleinden verwerkt, aangemerkt als verwerkingsverantwoordelijke voor die gegevens en is zij derhalve primair verantwoordelijk voor de naleving van de wettelijke vereisten. Wanneer wij bijvoorbeeld werkgever zijn, zijn wij de verwerkingsverantwoordelijke voor de persoonsgegevens van onze werknemers die wij verwerken.

Wanneer een organisatie daarentegen gegevens verwerkt namens een andere entiteit (bijvoorbeeld om een dienst te verlenen), wordt eerstgenoemde aangemerkt als verwerker van de gegevens.

HOE BEÏNVLOEDT DE EUROPESE WETGEVING INZAKE GEGEVENSBESCHERMING DE DOORGIFTE VAN PERSOONSGEGEVENS TUSSEN GROEPSLEDEN?

De Europese wetgeving inzake gegevensbescherming staat de doorgifte van persoonsgegevens niet toe naar landen, gebieden of internationale organisaties buiten Europa die geen passend beschermingsniveau waarborgen voor de rechten van natuurlijke personen op het gebied van gegevensbescherming. Aangezien sommige van de landen waarin Groepsleden actief zijn, door de Europese Commissie niet worden beschouwd als landen die een passend beschermingsniveau bieden, moeten passende waarborgen worden getroffen om te voldoen aan de vereisten van de Europese wetgeving inzake gegevensbescherming.

WELKE MAATREGELEN NEMEN DE GROEPSLEDEN HIERTEGEN?

Groepsleden moeten passende maatregelen nemen om te waarborgen dat zij bij de internationale doorgifte van persoonsgegevens deze gegevens op veilige en rechtmatige wijze verwerken. Het doel van dit Beleid is dan ook om een kader vast te leggen dat voldoet aan de normen zoals vastgelegd in de Europese wetgeving inzake gegevensbescherming en daarmee een passend beschermingsniveau te bieden voor alle persoonsgegevens die worden doorgegeven door Exporterende entiteiten aan Importerende entiteiten.

Dit Beleid is juridisch bindend en is van toepassing op alle Groepsleden en hun werknemers wanneer deze Groepsleden persoonsgegevens zowel handmatig als automatisch verwerken. Dit vereist dat Groepsleden voldoen aan de in Deel II van dit Beleid uiteengezette Regels (voor zover van toepassing), alsmede aan de in de bijlagen in Deel III van dit Beleid uiteengezette beleidsregels en procedures. Indien een Importerende entiteit onderworpen is aan een Toepasselijke lokale wetgeving inzake gegevensbescherming die wordt erkend als een wetgeving die een passend beschermingsniveau biedt volgens de Toepasselijke lokale wetgeving inzake gegevensbescherming van de Exporterende entiteit en die een beschermingsniveau biedt dat gelijkwaardig is aan hetgeen in dit Beleid is uiteengezet, zullen lokale processen en procedures die in wezen voldoen aan de vereisten van dit Beleid als geldig worden beschouwd, zelfs indien deze procedurele afwijkingen of verschillen inhouden (bijvoorbeeld lokale teams die bepaalde procedures afhandelen), mits dergelijke afwijkingen in overeenstemming zijn met dit Beleid. De internationale doorgiften waarop dit Beleid van toepassing is, omvatten doorgiften van persoonsgegevens van Groepsleden die onder het geografische toepassingsgebied van de AVG vallen overeenkomstig artikel 3 van de AVG, aan Groepsleden buiten de EER, alsmede verdere doorgiften aan andere Groepsleden of externe derden (conform de vereisten van regel 6 hieronder) buiten de EER.

WAT GEBEURT ER MET GROEPSLEDEN DIE NIET ONDER DE EUROPESE WETGEVING INZAKE GEGEVENSBESCHERMING VALLEN EN DIE GEGEVENS EXPORTEREN?

Zoals in de inleiding is uiteengezet, en met het oog op het opzetten van een wereldwijd kader voor gegevensbescherming voor de Santander Groep, geldt het volgende: indien een Groepslid dat niet onder de Europese wetgeving inzake gegevensbescherming valt, eveneens beperkingen kent met betrekking tot internationale doorgiften van persoonsgegevens krachtens de voor het betreffende land Toepasselijke lokale wetgeving inzake gegevensbescherming, en de lokale autoriteiten van die landen dit Beleid (geheel of gedeeltelijk, al naar gelang de vereisten van de Toepasselijke lokale wetgeving inzake gegevensbescherming) erkennen als een geldig mechanisme voor het legitimeren van internationale doorgiften van persoonsgegevens, dan kan dit Beleid ook van toepassing zijn op de persoonsgegevens die vanuit dergelijke landen aan de Importerende entiteiten worden doorgegeven. Ter verduidelijking: dit laat de toepassing van de Toepasselijke lokale wetgeving inzake gegevensbescherming op het Groepslid buiten Europa onverlet.

WELKE PERSOONSGEGEVENS VALLEN ONDER DIT BELEID?

De persoonsgegevens die in het kader van dit Beleid worden verwerkt, omvatten:

- Met betrekking tot de persoonsgegevens van **huidige en voormalige werknemers en overig personeel (zoals stagiairs, gedetacheerden of freelancers)**:

  (a) Persoons- en contactgegevens (zoals voornaam, tweede voornaam, achternaam, titel, alias, handtekening, geslacht, geboortedatum, nationaliteit, nationale identificatienummers/-documenten, e-mailadres, woonadres, telefoonnummers, foto, werkvergunningen enz.); **(b) Werkgerelateerde met inbegrip van arbeidsverleden, arbeidsvoorwaarden en contactgegevens** (zoals e-mailadres en telefoonnummer van het bedrijf, personeelsnummer, toewijzing van gebruikersnaam/adrescode (gebruikt voor toegang tot een werkstationterminal), arbeidsverleden, huidige functie, rol, taken, bedrijf, bedrijfscentrum, bedrijfsonderdeel, afdelingsnummer, vestigingsnummer, land van werkzaamheid, ID en naam van leidinggevende(n), ID en naam van ondergeschikte(n) , dienstverbandstatus en -type, of de werknemer extern is, indiensttredingsdatum, startdatum dienstverband, (indien van toepassing) einddatum dienstverband, contractgegevens, pensioenregelingen, flexibele werkregelingen, overplaatsingsverzoeken, schenkingen, gegevens inzake naleving van intern beleid of andere wettelijk toepasselijke voorschriften, prestatiebeoordelingen en -waarderingen (inclusief feedback van leidinggevenden, belanghebbenden en andere personen die met de werknemer samenwerken), promoties en disciplinaire maatregelen enz.); **(c) Gegevens inzake talent, werving en sollicitaties, opleiding en training** (zoals gegevens uit sollicitatiebrieven en cv's, gegevens over ontwikkelingsplannen en evaluaties, opleidingsgegevens, persoonlijke websites of LinkedIn-profielen die rechtstreeks door werknemers zijn verstrekt, eerdere werkervaring en referenties, opleidingsgeschiedenis, beroepskwalificaties, taalvaardigheden en andere relevante vaardigheden enz.); **(d) Financiële informatie, waaronder gegevens over loon en beloningen** (zoals bankrekeninggegevens, salaris, secundaire arbeidsvoorwaarden, bonussen, valuta's, variabele beloningen, gegevens over aandelenopties, toekenning van aandelen en andere beloningen, betalingsfrequentie, ingangsdatum van de huidige beloning, salarisbeoordelingen, belastingnummer en belastingcode enz.); **(e) Beveiligings- en IT-gegevens** (zoals gebruikers-ID, toegangssleutel voor tools, inloggegevens, beveiligingsgegevens en -profielen, e-mails die zijn verzonden vanuit en ontvangen op de e-mailaccounts van het bedrijf (voor zover wettelijk toegestaan), informatie die via IT-gebruik wordt vastgelegd, waaronder toegangs- en authenticatiegegevens, browsegeschiedenis op internet, gebelde telefoonnummers, documenten en bestanden die zijn opgeslagen op bedrijfssystemen of -netwerken (inclusief computerbureaubladen), logbestanden, IP-adres, geslaagde en mislukte inlogpogingen, informatie verzameld via cookies of andere soortgelijke trackingtechnologieën enz.); **(f) Werkroostergegevens** (zoals vakantiedagen, vrije dagen en vrije uren, overige verlofvormen en bewijs van de redenen daarvoor (indien van toepassing), data van terugkeer na verlof, overige afwezigheidsgegevens, registratie van gewerkte uren (voor zover wettelijk vereist of toegestaan), overuren, werkdiensten enz.); en en **(g) Alle andere informatie die door betrokkenen vrijwillig wordt verstrekt** (bijvoorbeeld via betrokkenheidsenquêtes of andere enquêtes enz.).

Daarnaast mogen **bijzondere categorieën persoonsgegevens** (**met name, maar niet uitsluitend, gezondheidsgegevens en gegevens over vakbondslidmaatschap**) door de Groepsleden worden verwerkt wanneer dit noodzakelijk is en krachtens de toepasselijke wetgeving is vereist of toegestaan voor de doeleinden die in de volgende sectie worden beschreven.

- Met betrekking tot de persoonsgegevens van **familieleden van werknemers**:

  (a) Persoons- en contactgegevens (zoals voornaam, achternaam, geslacht, nationale identificatienummers/-documenten, contactgegevens zoals een noodcontactnummer enz.); en **(b) Overige informatie over de werknemers of hun gezin, voor zover dit wettelijk vereist of toegestaan is** (zoals gezinssamenstelling en -situatie, relatie tot de werknemer, naam en andere relevante informatie over kinderen en andere afhankelijke personen, burgerlijke staat, gegevens inzake naleving van interne beleidsregels of andere wettelijk toepasselijke voorschriften enz.).

- Met betrekking tot de persoonsgegevens van **huidige en voormalige sollicitanten**:

  (a) Persoons- en contactgegevens (zoals voornaam, achternaam, land, provincie en woonplaats, e-mailadres, woonadres, telefoonnummers, nationaliteit enz.); **(b) Gegevens over werving, opleiding en training** (zoals gegevens uit sollicitatiebrieven en cv's, persoonlijke websites of LinkedIn-profielen die rechtstreeks door sollicitanten zijn verstrekt, eerdere werkervaring en referenties, opleidingsgeschiedenis, beroepskwalificaties, taal- en andere relevante vaardigheden, gegevens over beoordelingen in het kader van prestatiebeheer, ontwikkelingsplannen en bereidheid tot verhuizing, persoonsgegevens die voortvloeien uit de deelname van sollicitanten aan het wervingsproces, zoals bijvoorbeeld gegevens die zijn verkregen tijdens persoonlijke sollicitatiegesprekken en de e-mailcorrespondentie met betrekking tot sollicitaties of de gesprekken enz.); en **(c) Audio- en visuele informatie** (zoals stem en beeltenis zoals vastgelegd in foto-, video- of audio-opnamen in het kader van sollicitatiegesprekken die telefonisch of via videoconferentie zijn gevoerd enz.).

- Met betrekking tot de persoonsgegevens van **potentiële klanten, klanten en cliënten** (waaronder die van hun werknemers, vertegenwoordigers en/of agenten (voor zover van toepassing), geautoriseerde gebruikers en websitegebruikers):

  (a) Persoons- en contactgegevens (zoals voornaam, tweede voornaam, achternaam, telefoonnummer, e-mailadres, postadres, woonland, regio, staatsburgerschap of nationaliteit, nationale identificatienummers/-documenten, geslacht, taal, geboortedatum, geboorteland, burgerlijke staat, gegevens over gezins- of sociale omstandigheden (bijv. aantal afhankelijke personen), of de persoon minderjarig is of een wettelijke vertegenwoordiger nodig heeft, demografische en sociaal-economische gegevens enz.); **(b) Beroepsgegevens** (zoals beroep, functie, arbeids- en opleidingsverleden, bedrijfsgegevens, zakelijke contactgegevens, beroepscategorie, functietitel enz.); **(c) (Pre)contractuele gegevens** (zoals categoriecode, rechtsbevoegdheid, gegevens met betrekking tot volmachten, registratienummer en interne klantindicator, relatieniveau, zakelijke relatie met Santander, afgesloten of aangevraagde producten of diensten, risicoscore, informatie van kredietbureaus, inkooporders, statistische gegevens, facturen, informatie over goederen en activa, subsidies, rekening- en transactiegegevens, voor zover toegestaan door de toepasselijke wetgeving, contracten en andere overeenkomsten die persoonsgegevens kunnen bevatten met betrekking tot deze betrokkenen en hun prestaties enz.); **(d) Financiële, fiscale en betalingsgegevens** (zoals bankrekeninggegevens, gegevens van begunstigden, huidige en historische saldi van producten en diensten en betalingsgeschiedenis, creditcardgegevens, rechtstreekse salarisbetaling, inkomensgegevens/-type, beschikbare middelen, geldtransacties, betalingsbedrag, overboekingsgegevens, solvabiliteitsgegevens, fiscaal identificatienummer, fiscaal woonland, jaarlijks belastingsaldo enz.); **(e) Nalevingsgegevens** (zoals gekoppelde PEP-ID, MIFID of soortgelijke relatie (zoals zakenpartners, familiebanden enz.), relatietype (zoals echtgenoot/echtgenote, familielid, aandeelhouder, wettelijke vertegenwoordigers enz.),

startdatum en (indien van toepassing) einddatum van de relatie, informatie met betrekking tot verplichtingen inzake witwasbestrijding (AML) en fraudepreventie (profielen, informatie en scores uit solvabiliteits- en risicodatabases enz.); **(f) Audio- en visuele informatie** (zoals stem en beeltenis zoals vastgelegd in foto-, video- of audio-opnamen in het kader van vergaderingen die telefonisch of via videoconferentie zijn gevoerd, of die voor beveiligingsdoeleinden zijn gemaakt enz.); **(g) IT-informatie** (zoals IP-adres, gebruikers-ID, wachtwoorden, logboeken (inclusief profielgegevens) van de websites of portalen van de Santander Groep, toegangssleutels voor tools, beveiligingsgegevens en -profielen, IT-authenticatiegegevens, browsegeschiedenis, apparaat-ID, advertentie-ID, sociale netwerken enz.); en **(h) Overige gegevens over de professionele relatie met de Santander Groep** (zoals klachtgegevens, uitgewisselde communicatie, communicatievoorkeuren, verzoeken enz.).

Daarnaast mogen **bijzondere categorieën persoonsgegevens (met inbegrip van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten, in de context van internationale risico's en sancties**) door de Groepsleden worden verwerkt wanneer dit noodzakelijk is en krachtens de toepasselijke wetgeving is vereist of toegestaan voor de doeleinden die in de volgende sectie worden beschreven.

- Met betrekking tot de persoonsgegevens van **potentiële en huidige leveranciers, verkopers of dienstverleners** (waaronder die van hun werknemers, vertegenwoordigers en/of agenten, voor zover van toepassing):

  (a) Persoonsgegevens, professionele gegevens en contactgegevens (zoals voornaam, achternaam, telefoonnummer, e-mailadres, postadres, nationale identificatienummers/-documenten, functie/functietitel, bedrijfsgegevens, zakelijke contactgegevens enz.); **(b) Contractuele gegevens** (zoals gegevens met betrekking tot volmachten, inkooporders, facturen, contracten en andere overeenkomsten die persoonsgegevens over deze betrokkenen kunnen bevatten enz.); **(c) Financiële en betalingsgegevens** (zoals bankrekeninggegevens, creditcardgegevens, solvabiliteitsgegevens enz.); **(d) Audio- en visuele informatie** (zoals stem en beeltenis zoals vastgelegd in foto-, video- of audio-opnamen in het kader van vergaderingen die telefonisch of via videoconferentie zijn gevoerd, of die voor beveiligingsdoeleinden zijn gemaakt (inclusief informatie die wordt vastgelegd via toegangssystemen en beveiligingscamera's) enz.); **(e) IT-informatie** (zoals IP-adres, gebruikers-ID, wachtwoorden, logbestanden (waaronder profielgegevens) van websites of portalen van de Santander Groep enz.); en **(f) Overige gegevens over de professionele relatie met de Santander Groep** (zoals klachtgegevens, uitgewisselde communicatie enz.).

- Met betrekking tot de persoonsgegevens van **aandeelhouders**:

  (a) Persoonsgegevens, professionele gegevens en contactgegevens (zoals voornaam, achternaam, geslacht, geboortedatum, telefoonnummer, e-mailadres, postadres, nationale identificatienummers/-documenten, functie/functietitel, bedrijfsgegevens, zakelijke contactgegevens, aandeelhoudersnummer, nationaliteit/staatsburgerschap, geboorteland en woonland enz.); **(b) Financiële en betalingsgegevens** (zoals bankrekeninggegevens, creditcardgegevens, betalingsgegevens, aantal aandelen, eigendoms- en dividenddocumenten, geldtransacties, mutaties, posities en houders van aandelen in andere ondernemingen, informatie over afgesloten financiële producten enz.); en **(c) IT-informatie** (zoals IP-adres, gebruikers-ID, wachtwoorden, logbestanden (inclusief profielgegevens) van websites of portalen van de Santander Groep enz.).

- Met betrekking tot de persoonsgegevens van **webgebruikers, eindgebruikers en institutionele gebruikers (waaronder gebruikers van platforms, websites en apps die verband houden met universiteiten, de arbeidsmarkt en ondernemerschap)**:

(a) **Persoons- en contactgegevens** (zoals voornaam, achternaam, geboortedatum, geslacht, e-mailadres, postadres, telefoonnummers, woonland, nationaliteit, nationale identificatienummers enz.); **(b) Beroeps- en opleidingsgegevens** (zoals functie/functietitel, bedrijfsgegevens, zakelijke contactgegevens, arbeidsverleden, cv, academische gegevens, opleiding of kwalificaties, demografische en sociaaleconomische gegevens, betrekking met ondernemerschapsprojecten of bedrijven, enz.); **(c) IT-informatie** (zoals IP-adres, gebruikers-ID, wachtwoorden, logbestanden over het gebruik (inclusief profielgegevens) van websites of portalen, oproepregistraties enz.); **(d) Navigatie- en gebruiksgegevens** (zoals informatie van betrokkenen die automatisch wordt verzameld (d.w.z. via cookies of andere soortgelijke technologieën) met betrekking tot hun gebruik van websites en apparaten (inclusief profielen), browsen op het internet, gebruiksgegevens enz.); en **(e) Overige gegevens over hun relatie met de Santander Groep** (zoals vragen, interesses, uitgewisselde communicatie enz.)

VOOR WELKE DOELEINDEN WORDEN PERSOONSGEGEVENS KRACHTENS DIT BELEID DOORGEGEVEN?

Persoonsgegevens worden krachtens dit Beleid wereldwijd uitgewisseld tussen Groepsleden (voornamelijk Argentinië, de Bahama's, Brazilië, Colombia, Europese landen, Mexico, Peru, Zwitserland, het Verenigd Koninkrijk, de Verenigde Staten van Amerika, Uruguay enz.) voor de volgende doeleinden en uitsluitend voor zover dit krachtens de toepasselijke wetgeving is toegestaan:

- De doorgifte van persoonsgegevens van **huidige en voormalige werknemers en ander personeel (zoals stagiairs, gedetacheerden of freelancers)** vindt plaats ten behoeve van: **(a) het beheer en de administratie van personeel** (zoals opleidingsbeheer, planning en toezicht, prestatiebeheer, het beheer van lonen en secundaire arbeidsvoorwaarden, promoties, opvolgingsplanning en loopbaanontwikkeling, het regelen van interne mobiliteit, overplaatsingen en detacheringen, het samenstellen en beheren van bestaande personeelsregisters, het regelen van zakenreizen, het beheren van zakelijke onkosten en vergoedingen, het faciliteren van zakelijke communicatie, onderhandelingen, transacties en conferenties, het controleren van de nakoming van de arbeidsverplichtingen en -taken van de werknemer, verlof en afwezigheden, beoordelingen, het beheren van en rapporteren over tuchtzaken en beëindigingen van dienstverbanden, het toetsen van beslissingen inzake het dienstverband, het vaststellen van en het nemen van beslissingen met betrekking tot de geschiktheid van werknemers om te werken en aanpassingen van de werkplek, het toezicht op de naleving van interne beleidsregels en procedures en andere toezichtactiviteiten zoals vereist door de toepasselijke wetgeving (zoals interne meldingssystemen), waaronder naleving van de Gedragscode voor de Effectenmarkten of soortgelijke beleidsregels en daarmee samenhangende verplichtingen, waaronder de goedkeuring van en het toezicht op transacties via persoonlijke rekeningen, het uitvoeren van personeelsanalyses en -planning, het uitvoeren van antecedentenonderzoeken zoals vereist of toegestaan door toepasselijke wetgeving enz.); **(b) het uitvoeren van geaggregeerde segmentaties, statistieken en analyses** met betrekking tot activiteitsgegevens van werknemers teneinde het inzicht in de werknemerspopulatie te verbeteren en de besluitvorming hierover te onderbouwen, onder meer met betrekking tot het werven van talent, loopbaanplanning en opvolgingsplanning; **(c) het ondersteunen van het beheer van de door de Santander Groep geleverde diensten en haar bedrijfsactiviteiten** (zoals het beheren en beveiligen van IT- en communicatiesystemen en -infrastructuur, het beheren en toewijzen van bedrijfsmiddelen en personeel, kantoorapparatuur en andere eigendommen, operationele en strategische planning, projectbeheer, bedrijfscontinuïteit, het samenstellen van audittrails en andere rapportagetools, het bijhouden van gegevens met betrekking tot bedrijfsactiviteiten, budgettering, financieel beheer en rapportage, communicatie, het beheer van fusies, overnames en reorganisaties of afstotingen enz.); en **(d) het naleven van toepasselijke wettelijke verplichtingen en andere vereisten** (zoals verplichtingen inzake gegevensbescherming, belasting- en socialezekerheidswetgeving, risicopreventie en arbeidswetgeving, fraudepreventie, klokkenluidersregeling, verplichtingen inzake het bijhouden van gegevens en rapportage, het uitoefenen van wettelijke rechten en rechtsmiddelen, het voeren van rechtszaken, het waarborgen van naleving bij overheidsinspecties en andere verzoeken van de overheid of andere overheidsinstanties, het reageren

op juridische procedures zoals dagvaardingen, verplichtingen op het gebied van arbeid en sociale zekerheid, het uitvoeren van audits en het afhandelen van interne klachten of vorderingen enz.).

Met betrekking tot **bijzondere categorieën persoonsgegevens van werknemers (met inbegrip van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten, voor zover toegestaan)**, kunnen deze gegevens door de Groepsleden worden verwerkt indien dit noodzakelijk is om de doeleinden daarvan naar behoren te verwezenlijken (zoals het nakomen van wettelijke verplichtingen, personeelsbeheer, het beheer van klokkenluiderskanalen, het beheer van lonen en secundaire arbeidsvoorwaarden, het beheer van interne mobiliteit, overplaatsingen en detacheringen, het uitvoeren van geaggregeerde segmentaties, statistieken en analyses enz.) en uitsluitend voor zover dit noodzakelijk is voor het nakomen van de verplichtingen en het uitoefenen van specifieke rechten van Groepsleden of van de betrokkene op het gebied van arbeidsrecht en socialezekerheids- en sociale-beschermingsrecht (artikel 9, lid 2, onder b), AVG) en voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnose, het verlenen van gezondheids- of sociale zorg of behandeling, of het beheer van gezondheids- of sociale zorgstelsels en -diensten (artikel 9, lid 2, onder h), AVG).

- De doorgifte van persoonsgegevens van **familieleden van werknemers** vindt plaats ten behoeve van het beheer van de overplaatsing van werknemers naar het buitenland, het uitvoeren van geaggregeerde segmentaties, statistieken en analyses, evenals het toezicht op de naleving van de Gedragscode voor de Effectenmarkten of soortgelijke beleidsregels en daarmee samenhangende verplichtingen, waaronder de goedkeuring van en het toezicht op transacties via persoonlijke rekeningen, alsook het beheer van sociale voorzieningen met betrekking tot de rechten van werknemers (bijvoorbeeld in de context van verzekeringen).

- De doorgifte van persoonsgegevens van **huidige en voormalige sollicitanten** vindt plaats ten behoeve van het beheer van nationale en internationale wervingsactiviteiten (zoals het beoordelen van sollicitaties en het nemen van beslissingen over aanstellingen, het communiceren met sollicitanten in verband met het wervingsproces en/of hun sollicitatie(s) enz.).

- De doorgifte van persoonsgegevens van **potentiële klanten, klanten en cliënten**(waaronder die van hun werknemers, vertegenwoordigers en/of agenten, geautoriseerde gebruikers en internetgebruikers) vindt plaats ten behoeve van: **(a) het beheren van de contractuele relatie met hen en het leveren van onze diensten** (zoals het uitgeven van betaalkaarten, waaronder aan geautoriseerde gebruikers via een bedrijfskaart, het aanbieden en beheren van onze betalingsdiensten en online bankdiensten, het bijhouden van gegevens om de afstemming van informatie tussen verschillende rechtsgebieden te waarborgen, het sluiten van overeenkomsten en/of het nemen van stappen om dergelijke overeenkomsten aan te gaan (KYC-processen), voor zakelijke doeleinden en communicatie, het overboeken van rekeningen, het aangaan, verlengen, onderhouden of beëindigen van de zakelijke relaties, het verlenen van toegang tot activiteiten op internet en onze bedrijfsruimten, het bijhouden van bedrijfsadministratie, het uitvoeren van audits, boekhouding, financiële en economische analyses, het uitvoeren van betalings- en daarmee samenhangende boekhoudkundige taken, risico- en krediet-/solvabiliteitsbeoordelingen enz.); **(b) het beheren en waarborgen van de beveiliging** (zoals het beveiligen van IT-infrastructuur, kantoorapparatuur en andere eigendommen enz.); **(c) het beheren van de bedrijfsvoering**(zoals het bijhouden van gegevens over vertegenwoordigers van bedrijven of andere contactpersonen, het waarborgen van afstemming van de bedrijfsvoering tussen verschillende rechtsgebieden, het bijhouden van verslagen van vergaderingen en andere zakelijke relaties, het exploiteren en beheren van de IT- en communicatiesystemen, het beheren van de ontwikkeling van producten en diensten, het verbeteren van producten en diensten, het beheren van bedrijfsactiva, strategische planning, projectbeheer, bedrijfscontinuïteit, het samenstellen van audittrails en andere rapportagetools enz.); **(d) het naleven van de toepasselijke wetgeving** (zoals verplichtingen op het gebied van gegevensbescherming en belastingen, MiFID en de geschiktheid en gepastheid van

beleggingsproducten, fraudepreventie, bestrijding van witwassen, verplichtingen inzake het bijhouden van gegevens en rapportage, het uitoefenen van wettelijke rechten en rechtsmiddelen, het voeren van verdediging in geschillen of rechtszaken, het waarborgen van naleving bij overheidsinspecties en andere verzoeken van de overheid of andere overheidsinstanties, het reageren op juridische procedures zoals dagvaardingen enz.); en **(e) het plannen en uitvoeren van marketingstrategieën of -campagnes** (bijv. marketingonderzoek, het plannen van campagnes en het ontwikkelen van marketingstrategieën, het monitoren van en rapporteren over het succes van campagnes, het afstemmen van producten/diensten op specifieke doelgroepen (inclusief profilering), voor zover hiervoor toestemming is verleend of dit wettelijk is toegestaan enz.).

Met betrekking tot klanten en cliënten (met inbegrip van die van hun werknemers, vertegenwoordigers en/of agenten) en hun **bijzondere categorieën persoonsgegevens (met inbegrip van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten, voor zover toegestaan**) kunnen deze gegevens door de Groepsleden worden verwerkt indien dit noodzakelijk is om de doeleinden daarvan naar behoren te verwezenlijken (zoals het nakomen van wettelijke verplichtingen, het identificeren van openbaar beschikbare informatie over praktijken van cliënten van andere entiteiten die van invloed kunnen zijn op hun relatie met het bedrijf; het waarborgen van de afstemming van informatie tussen verschillende rechtsgebieden, het voldoen aan overheids- of gerechtelijke inspecties en andere verzoeken van overheidsinstanties, enz.) en uitsluitend voor zover dit noodzakelijk is voor het nakomen van de verplichtingen van de Groepsleden of van de betrokkene op het gebied van de bestrijding van witwassen, fraudepreventie, misdaadpreventie en aanverwante terreinen (indien noodzakelijk en vereist of toegestaan door de toepasselijke wetgeving).

- De doorgifte van persoonsgegevens van **potentiële en huidige leveranciers, verkopers of dienstverleners** (waaronder die van hun werknemers, vertegenwoordigers en/of agenten) vindt plaats ten behoeve van: **(a) het beheren van de (pre)contractuele relatie met hen of hun bedrijf** (indien het rechtspersonen betreft) **in het algemeen** (zoals het uitvoeren van controles op kwaliteitsnormen, het analyseren van het risiconiveau van dienstverleners, boekhoudkundige, financiële en economische analyses, het nemen van maatregelen om relevante overeenkomsten aan te gaan, het uitvoeren van bestaande overeenkomsten, het verrichten van betalingen en daarmee samenhangende boekhoudkundige taken, voor zakelijke doeleinden en communicatie, het aangaan, verlengen, onderhouden of beëindigen van de zakelijke relaties, het bijhouden van bedrijfsgegevens enz.); **(b) het beheren en waarborgen van de beveiliging** (zoals het beveiligen van de IT-infrastructuur, kantoorapparatuur en andere eigendommen enz.); **(c) het beheren van de bedrijfsvoering** (zoals het exploiteren en beheren van de IT- en communicatiesystemen, het beheren van de ontwikkeling van producten en diensten, strategische planning, projectbeheer, bedrijfscontinuïteit, het samenstellen van audittrails en andere rapportagetools, het bijhouden van gegevens met betrekking tot bedrijfsactiviteiten, budgettering, financieel beheer en rapportage, communicatie enz.); en **(d) het naleven van de toepasselijke wetgeving** (zoals verplichtingen op het gebied van handelsrecht, belastingrecht, fraudepreventie en uitbesteding wanneer deze door financiële instellingen worden uitgevoerd, het uitvoeren van audits, het voldoen aan overheidsinspecties en andere verzoeken van de overheid of andere overheidsinstanties, het uitoefenen van wettelijke rechten en rechtsmiddelen, het voeren van rechtszaken en het afhandelen van interne klachten of vorderingen enz.).

- De doorgifte van persoonsgegevens van **aandeelhouders** vindt plaats ten behoeve van: **(a) het beheren van de relatie met de aandeelhouder** (zoals voor zakelijke doeleinden en communicatie, het aangaan, vernieuwen, onderhouden of beëindigen van zakelijke relaties, het beheren van jaarvergaderingen en aandeelhoudersrechten, de uitkering van dividenden, het bijhouden van bedrijfsadministratie, het verlenen van toegang tot internetgebaseerde activiteiten en bedrijfsruimten, enz.); en **(b) het naleven van de toepasselijke wetgeving** (zoals handels- en vennootschapsrecht, belasting- en effectenwetgeving, het uitvoeren van audits, het voldoen aan overheidsinspecties en andere verzoeken van de overheid of andere overheidsinstanties, het nakomen van verplichtingen inzake de bestrijding

van witwassen, certificeringen, het uitoefenen van wettelijke rechten en rechtsmiddelen, het voeren van rechtszaken en het afhandelen van interne klachten of vorderingen enz.

- De doorgifte van persoonsgegevens van **webgebruikers, eindgebruikers en institutionele gebruikers (waaronder gebruikers van platforms, websites en apps die verband houden met universiteiten, de arbeidsmarkt en ondernemerschap)** vindt plaats ten behoeve van: **(a) het beheer van de dienstverlening in het algemeen** (zoals het ontwikkelen en aanbieden van onlinefuncties en -inhoud, het beheren van websites, het afhandelen van vragen en verzoeken, het bieden van ondersteuning enz.); **(b) het beheren en waarborgen van de beveiliging** (zoals het beveiligen van IT-infrastructuur, het waarborgen van de veiligheid en integriteit van systemen, servers en websites enz.); **(c) het beheren van de bedrijfsvoering** (zoals het waarborgen van afstemming van de bedrijfsvoering tussen verschillende rechtsgebieden, het bijhouden van verslagen van vergaderingen en andere zakelijke relaties, het wereldwijd verbeteren van processen op het gebied van personeelszaken en talentwerving enz.); **(d) het plannen en uitvoeren van marketingstrategieën of -campagnes** (zoals marktonderzoek, het plannen van campagnes en het ontwikkelen van marketingstrategieën, het monitoren van en rapporteren over het succes van campagnes, het afstemmen van producten/diensten op doelgroepen (inclusief profilering), voor zover hiervoor toestemming is verleend of dit wettelijk is toegestaan enz.); **(e) het beheren van nationale en internationale wervingsactiviteiten** (zoals het beoordelen van sollicitaties en het nemen van beslissingen over aanstellingen, het communiceren met sollicitanten met betrekking tot het wervingsproces en/of hun sollicitatie(s) enz.); **(f) het uitvoeren van geaggregeerde segmentaties, statistieken en analyses** (zoals inzicht verkrijgen in hoe de diensten worden gebruikt, het verbeteren en ontwikkelen van functionaliteiten van websites en diensten, het verbeteren van de prestaties en beschikbare ondersteuning enz.); en **(g) het naleven van de toepasselijke wetgeving** (zoals handelswetgeving, het uitvoeren van audits, het voldoen aan overheidsinspecties en andere verzoeken van de overheid of andere overheidsinstanties, het reageren op juridische procedures zoals dagvaardingen, het uitoefenen van wettelijke rechten en rechtsmiddelen, het voeren van rechtszaken en het afhandelen van interne klachten of vorderingen enz.).

De in dit Beleid genoemde persoonsgegevens worden eveneens tussen Groepsleden uitgewisseld voor zover nodig voor de **levering van een breed scala aan interne diensten tussen deze Groepsleden** (bijv. IT-technologie en -systemen, backoffice-diensten, werving en personeelsbeheer, interne audit en compliance, beheer van het klokkenluiderskanaal, centrale postdienst voor sollicitaties en medewerkers, betalingstechnologie en verwerkingsdiensten, autorisatie- en verwerkingsdiensten voor creditcards, facturerings- en prijsbepalingsdiensten, documentvernietiging, documenttransport, risicobeheer, inkoop van producten en/of diensten, elektronische facturering, beheer van marketing en communicatie, alsmede juridische beheer- en coördinatiediensten op bepaalde gebieden zoals gegevensbescherming enz.)

MEER INFORMATIE

De Santander Groep heeft lokale functionarissen voor gegevensbescherming (FG's) en/of contactpersonen (‘Champions’) aangesteld (zoals deze termen hieronder zullen worden gedefinieerd) die leiding geven aan de lokale teams en toezien op de naleving van de lokale regelgeving binnen verschillende entiteiten wereldwijd, en die deel uitmaken van het Privacyteam van de Santander Groep (eveneens hieronder gedefinieerd). Indien u vragen hebt over de bepalingen van dit Beleid, uw rechten krachtens dit Beleid of andere kwesties inzake gegevensbescherming, kunt u contact opnemen met de betreffende FG of Champion via het hieronder vermelde adres. De FG of Champion zal ofwel de kwestie zelf afhandelen, ofwel deze doorsturen naar de juiste persoon of afdeling binnen de Santander Groep, ofwel, indien van toepassing, de kwestie escaleren naar de desbetreffende persoon of de desbetreffende instantie.

Ter attentie van: Privacyteam

E-mailadres: Een lijst met de relevante e-mailadressen vindt u hier.

Indien u zich zorgen maakt over de wijze waarop een Groepslid uw persoonsgegevens mogelijk heeft verwerkt, is er een specifieke Procedure voor klachtenafhandeling. Deze staat beschreven in Deel III (zie **Bijlage 2**).

DEEL II: VERPLICHTINGEN VAN GROEPSLEDEN

Deel II van dit Beleid is onderverdeeld in drie secties:

- Sectie A behandelt de basisbeginselen inzake gegevensbescherming die overeenkomen met die uit de Europese wetgeving inzake gegevensbescherming en die een Groepslid moet naleven.

- Sectie B behandelt de door Groepsleden aangegane praktische verplichtingen jegens de bevoegde toezichthoudende autoriteiten in verband met dit Beleid.

- Sectie C beschrijft de rechten van derde-begunstigden die Groepsleden krachtens Deel II van dit Beleid aan betrokkenen hebben toegekend.

SECTIE A: BASISBEGINSELEN

REGEL 1 – RECHTMATIGHEID EN EERLIJKHEID

Regel 1A – Groepsleden dienen dit Beleid en alle Toepasselijke lokale wetgeving inzake gegevensbescherming op een geharmoniseerde wijze na te leven.

Als organisaties zullen Groepsleden, met inachtneming van het hieronder vermelde, alle toepasselijke wetgeving met betrekking tot persoonsgegevens (bijvoorbeeld in Europa, de Europese wetgeving inzake gegevensbescherming) naleven en ervoor zorgen dat, wanneer persoonsgegevens worden verwerkt, dit gebeurt in overeenstemming met dit Beleid en de Toepasselijke lokale wetgeving inzake gegevensbescherming.

Waar dit Beleid van toepassing is en:

- er geen Toepasselijke lokale wetgeving inzake gegevensbescherming bestaat, of de wetgeving niet voldoet aan de normen die zijn vastgelegd in de regels van dit Beleid, zullen de Groepsleden persoonsgegevens verwerken overeenkomstig dit Beleid en met inachtneming van de regels die in dit Beleid zijn vastgelegd;

- de Toepasselijke lokale wetgeving inzake gegevensbescherming een hoger beschermingsniveau vereist dan waarin dit Beleid voorziet, zal het hogere beschermingsniveau voorrang hebben boven dit Beleid, mits de rechten en verplichtingen uit hoofde van dit Beleid blijven worden nageleefd; of

- de Toepasselijke lokale wetgeving inzake gegevensbescherming Groepsleden belet hun verplichtingen uit hoofde van dit Beleid na te komen, of een wezenlijke invloed heeft op hun vermogen om hieraan te voldoen, zullen Groepsleden de procedure volgen die is uiteengezet in Regel 13.

Regel 1B – Groepsleden dienen ervoor te zorgen dat hun verwerking van persoonsgegevens eerlijk en rechtmatig is en dat er, indien vereist, een rechtsgrondslag bestaat voor de verwerking van persoonsgegevens.

Groepsleden zullen ervoor zorgen dat hun verwerking van persoonsgegevens eerlijk en rechtmatig is, en dat er, indien vereist, een rechtsgrondslag bestaat voor de verwerking van persoonsgegevens. In overeenstemming met de Europese wetgeving inzake gegevensbescherming verwerken Groepsleden alleen persoonsgegevens wanneer:

- de betrokkene toestemming heeft gegeven voor de verwerking van zijn of haar persoonsgegevens en die toestemming voldoet aan de vereiste normen krachtens de Europese wetgeving inzake

gegevensbescherming (d.w.z. dat deze vrijwillig, specifiek, geïnformeerd en ondubbelzinnig moet zijn); of

- dit noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene maatregelen te nemen alvorens een overeenkomst aan te gaan; of

- dit noodzakelijk is om te voldoen aan een wettelijke verplichting waaraan het Groepslid is onderworpen (voor zover die wet voldoet aan de vereisten krachtens Regel 13 hieronder, indien van toepassing); of

- dit noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon; of

- dit noodzakelijk is voor de uitvoering van een taak die wordt uitgevoerd in het algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan een Groepslid is toevertrouwd (voor zover deze taak is vastgelegd in een wet die voldoet aan de vereisten krachtens Regel 13 hieronder, indien van toepassing); of

- dit noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van een Groepslid of van een derde, tenzij de belangen of de grondrechten en fundamentele vrijheden van de betrokkene zwaarder wegen dan die belangen.

Wanneer de verwerking van persoonsgegevens betrekking heeft op strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen, zullen Groepsleden een dergelijke verwerking alleen uitvoeren onder toezicht van een overheidsinstantie, of indien de verwerking is toegestaan op grond van een wet die voorziet in passende waarborgen voor de rechten en vrijheden van betrokkenen in overeenstemming met de hierboven genoemde rechtsgrondslagen.

Regel 1C – Onverminderd het bepaalde in Regel 1B hierboven, is de verwerking van bijzondere categorieën persoonsgegevens verboden, tenzij een uitzondering, zoals vastgelegd in de Europese wetgeving inzake gegevensbescherming, van toepassing is.

De verwerking van bijzondere categorieën persoonsgegevens is alleen toegestaan op bepaalde gronden:

- Het Groepslid heeft uitdrukkelijke toestemming verkregen voor de verwerking van bijzondere categorieën persoonsgegevens die betrekking hebben op de betrokkene voor één of meer gespecificeerde doeleinden, tenzij een wet bepaalt dat het verbod op de verwerking van bijzondere categorieën persoonsgegevens niet door de betrokkene kan worden opgeheven; of

- De verwerking is noodzakelijk voor het nakomen van de verplichtingen en het uitoefenen van specifieke rechten van het Groepslid of van de betrokkene op het gebied van het arbeidsrecht en de wetgeving inzake sociale zekerheid en sociale bescherming, voor zover dit is toegestaan door de wet of een collectieve overeenkomst op grond van de wet die voorziet in passende waarborgen voor de grondrechten en belangen van betrokkenen; of

- De verwerking is noodzakelijk ter bescherming van de vitale belangen van een betrokkene of van een andere natuurlijke persoon, wanneer de betrokkene fysiek of juridisch niet in staat is toestemming te geven; of

- De verwerking wordt uitgevoerd in het kader van rechtmatige activiteiten, met passende waarborgen, door een stichting, vereniging of enige andere organisatie zonder winstoogmerk met een politiek,

filosofisch, religieus of vakbondsdoel, op voorwaarde dat de verwerking uitsluitend betrekking heeft op de leden of voormalige leden van de organisatie of op personen die in verband met de doelstellingen ervan regelmatig contact met haar hebben, en dat de persoonsgegevens niet buiten die organisatie worden bekendgemaakt zonder toestemming van de betrokkenen; of

- De verwerking heeft betrekking op persoonsgegevens die door de betrokkene kennelijk openbaar zijn gemaakt; of

- De verwerking is noodzakelijk voor de vaststelling, uitoefening of verdediging van rechtsvorderingen, of wanneer rechtbanken in hun gerechtelijke hoedanigheid optreden; of

- De verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang op grond van een wet, mits deze evenredig is aan het nagestreefde doel, de essentie van gegevensbescherming eerbiedigt en voorziet in passende en specifieke maatregelen ter waarborging van de grondrechten en belangen van de betrokkene; of

- De verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, voor medische diagnose, voor het verlenen van gezondheids- of sociale zorg of behandeling, of voor het beheer van gezondheids- of sociale zorgstelsels en -diensten op grond van een wet, mits de verwerking wordt uitgevoerd door of onder de verantwoordelijkheid van een beroepsbeoefenaar die onderworpen is aan geheimhoudingsplichten krachtens een wet of krachtens regels die zijn vastgesteld door bevoegde nationale instanties; of

- De verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid op grond van een wet die voorziet in passende en specifieke maatregelen ter waarborging van de rechten en vrijheden van de betrokkenen, in het bijzonder beroepsgeheim; of

- De verwerking is noodzakelijk voor archiveringsdoeleinden in het algemeen belang, voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden op grond van een wet die in verhouding staat tot het nagestreefde doel, de essentie van het recht op gegevensbescherming eerbiedigt en voorziet in passende en specifieke maatregelen ter waarborging van de grondrechten en de belangen van de betrokkene.

Regel 1D – Groepsleden dienen de gevolgen te beoordelen van elke verwerking van persoonsgegevens die hoge risico's met zich meebrengt voor de rechten en vrijheden van betrokkenen.

Exporterende entiteiten zullen, wanneer zij als verwerkingsverantwoordelijken optreden, de noodzaak en evenredigheid van elke nieuwe verwerking van persoonsgegevens beoordelen, en indien deze hoge risico's met zich meebrengt voor de rechten en vrijheden van betrokkenen, zullen zij een gegevensbeschermingseffectbeoordeling uitvoeren in overeenstemming met de Europese wetgeving inzake gegevensbescherming. Indien uit de gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico voor de betrokkenen met zich meebrengt, zijn de Exporterende entiteiten verplicht om, bij gebrek aan maatregelen ter beperking van het risico, de bevoegde toezichthoudende autoriteiten te raadplegen alvorens met de verwerking te beginnen.

REGEL 2 – HET WAARBORGEN VAN TRANSPARANTIE EN HET UITSLUITEND VERWERKEN VAN PERSOONSGEGEVENS VOOR EEN BEKEND DOEL

Regel 2A – Groepsleden dienen betrokkenen te informeren over de wijze waarop hun gegevens worden verwerkt.

Groepsleden zullen ervoor zorgen dat betrokkenen altijd op een duidelijke en volledige manier (gewoonlijk door middel van een verklaring inzake eerlijke verwerking) worden geïnformeerd over de wijze waarop hun persoonsgegevens zullen worden verwerkt. Het betreffende Groepslid zal informatie verstrekken in overeenstemming met de vereisten van de Europese wetgeving inzake gegevensbescherming. Deze informatie omvat ten minste het volgende:

- de identiteit en contactgegevens van de verwerkingsverantwoordelijke, met inbegrip van de contactgegevens van de functionaris voor gegevensbescherming en van de vertegenwoordiger, in voorkomend geval;

- het doel en de rechtsgrondslag voor de verwerking, met inbegrip van een toelichting op eventuele verwerking op basis van gerechtvaardigde belangen en eventuele nieuwe of andere verenigbare doeleinden;

- de ontvangers of categorieën ontvangers van de persoonsgegevens;

- informatie over de waarborgen die zijn getroffen ter bescherming van persoonsgegevens bij internationale doorgifte en hoe u toegang kunt krijgen tot of een kopie kunt verkrijgen van deze waarborgen. In het geval van doorgifte van persoonsgegevens tussen een Exporterende entiteit en een Importerende entiteit op basis van dit Beleid, zal de verstrekte informatie een verwijzing naar dit Beleid bevatten en zal worden vermeld hoe u dit Beleid kunt raadplegen;

- de termijn gedurende welke de persoonsgegevens worden bewaard of de criteria die worden gehanteerd om die termijn te bepalen;

- nadere informatie over de rechten van betrokkenen, waaronder het recht op inzage, rectificatie, verwijdering, beperking, bezwaar, gegevensoverdraagbaarheid, het recht om toestemming in te trekken (wanneer de verwerking op toestemming is gebaseerd) en het recht om een klacht in te dienen bij een toezichthoudende autoriteit;

- of het verstrekken van de informatie een wettelijke of contractuele verplichting is, en de gevolgen van het niet verstrekken van persoonsgegevens in dergelijke omstandigheden; en

- informatie over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en ten minste in gevallen waarin dergelijke beslissingen rechtsgevolgen hebben voor de betrokkene of deze op vergelijkbare wijze aanzienlijk beïnvloeden, of zijn gebaseerd op bijzondere categorieën persoonsgegevens, zinvolle informatie over de toegepaste logica, alsook de betekenis en de beoogde gevolgen van een dergelijke verwerking voor de betrokkene.

De vereisten van de Toepasselijke lokale wetgeving inzake gegevensbescherming in het land waar de persoonsgegevens worden verzameld, bepalen of er aanvullende informatie aan de betrokkenen moet worden verstrekt.

Deze informatie wordt verstrekt wanneer de Groepsleden de persoonsgegevens rechtstreeks van de betrokkene verkrijgen, of binnen een termijn die anderszins is toegestaan krachtens de Europese wetgeving inzake gegevensbescherming.

Wanneer Groepsleden de persoonsgegevens van een betrokkene verkrijgen uit een andere bron dan die betrokkene zelf, zal het desbetreffende Groepslid deze informatie aan de betrokkene verstrekken, samen met informatie over de bron en de categorieën persoonsgegevens die van derden zijn ontvangen, en wel als volgt:

- binnen een redelijke termijn na het verzamelen van de persoonsgegevens, maar uiterlijk binnen één (1) maand;
- indien de persoonsgegevens worden verwerkt met het oog op communicatie met de betrokkene, uiterlijk op het moment van de eerste communicatie met die betrokkene; of
- indien de persoonsgegevens aan een derde partij worden verstrekt, uiterlijk op het moment waarop de gegevens voor het eerst worden verstrekt.

Groepsleden dienen deze Regel 2A na te leven, tenzij het niet verstrekken van informatie uitdrukkelijk is toegestaan krachtens de Europese wetgeving inzake gegevensbescherming.

Regel 2B – Groepsleden mogen persoonsgegevens alleen verkrijgen en verwerken voor die doeleinden die bij de betrokkene bekend zijn, of die in overeenstemming zijn met de verwachtingen van de betrokkene en relevant zijn voor Groepsleden.

Regel 1A bepaalt dat Groepsleden dienen te voldoen aan alle toepasselijke wetgeving inzake de verwerking van persoonsgegevens (mits die wetgeving, voor zover van toepassing, voldoet aan de vereisten krachtens Regel 13 hieronder). Dit houdt in dat Groepsleden persoonsgegevens zullen verzamelen voor specifieke, uitdrukkelijk omschreven en legitieme doeleinden en die persoonsgegevens niet verder zullen verwerken op een wijze die onverenigbaar is met die doeleinden.

Groepsleden zullen de doeleinden waarvoor persoonsgegevens worden verwerkt (met inbegrip van het secundaire gebruik en de openbaarmaking van de gegevens) vaststellen en bekendmaken in overeenstemming met Regel 2A.

Regel 2C – Groepsleden mogen persoonsgegevens alleen verwerken voor een ander of nieuw doel indien dit verenigbaar is met het doel waarvoor deze zijn verzameld.

Indien een Groepslid persoonsgegevens verzamelt voor een specifiek doel overeenkomstig Regel 2A (zoals aan de betrokkene meegedeeld via de betreffende verklaring inzake eerlijke verwerking) en zoals beschreven in Regel 2B, en het Groepslid vervolgens persoonsgegevens voor een ander of nieuw doel wil verwerken, zal het die persoonsgegevens niet verder verwerken op een wijze die onverenigbaar is met het doel waarvoor ze zijn verzameld, tenzij een dergelijke verdere verwerking is gebaseerd op de toestemming van de betrokkene of wettelijk verplicht is (mits die wetgeving, voor zover van toepassing, voldoet aan de vereisten krachtens Regel 13 hieronder).

REGEL 3 – HET WAARBORGEN VAN DE GEGEVENSKWALITEIT

Regel 3A – Groepsleden dienen persoonsgegevens nauwkeurig en actueel te houden.

Om te waarborgen dat de persoonsgegevens waarover Groepsleden beschikken, nauwkeurig en actueel zijn, moedigen Groepsleden betrokkenen actief aan om hen te informeren wanneer hun persoonsgegevens wijzigen. Groepsleden zullen redelijke maatregelen nemen om ervoor te zorgen dat onjuiste persoonsgegevens, in het licht van de doeleinden waarvoor deze worden verwerkt, onverwijld worden gewist of gerectificeerd.

Regel 3B – Groepsleden mogen persoonsgegevens slechts zo lang als nodig is bewaren voor de doeleinden waarvoor deze worden verwerkt.

Groepsleden zullen zich houden aan de voor elk Groepslid geldende regelgeving en aan de beleidsregels en procedures van de Santander Groep inzake het bewaren van gegevens, zoals deze van tijd tot tijd worden herzien en bijgewerkt. Dit houdt onder meer in dat Groepsleden, al naar gelang het geval, persoonsgegevens verwijderen of afschermen die niet langer nodig zijn voor het doel waarvoor deze zijn verzameld en verder verwerkt.

Regel 3C – Groepsleden mogen alleen persoonsgegevens verwerken die toereikend en relevant zijn en beperkt blijven tot hetgeen noodzakelijk is in verhouding tot de doeleinden waarvoor zij worden verwerkt.

Groepsleden verwerken uitsluitend persoonsgegevens die noodzakelijk zijn om de doeleinden waarvoor zij worden verwerkt naar behoren te kunnen verwezenlijken.

REGEL 4 – HET TREFFEN VAN PASSENDE BEVEILIGINGSMAATREGELEN

Regel 4A – Groepsleden dienen het IT-beveiligingsbeleid van de Santander Groep na te leven.

Groepsleden zullen passende technische en organisatorische maatregelen treffen om persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging of verlies, wijziging, ongeoorloofde openbaarmaking of toegang, met name wanneer de verwerking gepaard gaat met de doorgifte van persoonsgegevens via een netwerk, en tegen alle andere onrechtmatige vormen van verwerking. Daartoe zullen de Groepsleden voldoen aan de vereisten van het binnen de Santander Groep geldende beveiligingsbeleid, zoals van tijd tot tijd herzien en bijgewerkt, alsmede aan alle andere beveiligingsprocedures die relevant zijn voor een bepaald bedrijfsonderdeel of een bepaalde functie. Rekening houdend met de stand van de techniek en de kosten van de implementatie daarvan, moeten deze maatregelen een beveiligingsniveau waarborgen dat in verhouding staat tot de risico's die de verwerking met zich meebrengt en de aard van de te beschermen gegevens.

Regel 4B – Groepsleden dienen een beleid inzake melding van inbreuken op de gegevensbeveiliging te hebben geïmplementeerd.

Groepsleden hebben procedures voor het reageren op inbreuken op de beveiliging van persoonsgegevens ingevoerd (die van tijd tot tijd worden herzien en bijgewerkt), waarin de werkwijze wordt beschreven die moet worden gevolgd in het geval van een inbreuk op de beveiliging die leidt tot de onopzettelijke of onrechtmatige vernietiging, het verlies, de wijziging, de ongeoorloofde openbaarmaking van of toegang tot persoonsgegevens die worden verzonden, opgeslagen of anderszins verwerkt (een "**Inbreuk op de persoonsgegevens**").

In het bijzonder zal, in geval van een Inbreuk op de persoonsgegevens, de persoon die binnen het betreffende Groepslid kennis neemt van de inbreuk, dit onverwijld melden aan:

- de betreffende functionaris voor gegevensbescherming (FG) of Champion, via de functie voor operationele risicobeheersing (indien van toepassing);
- het Groepslid dat optreedt als verwerkingsverantwoordelijke, wanneer het desbetreffende Groepslid optreedt als verwerker; en
- aan het Aansprakelijke BCR-lid.

De betreffende functionaris voor gegevensbescherming (DPO) of Champion zal, waar nodig met hulp van het Corporate DP Office, beoordelen of de Inbreuk op de persoonsgegevens moet worden gemeld aan de bevoegde toezichthoudende autoriteit. Indien dit het geval is, zal de betreffende FG of de Champion, al naar gelang de situatie, de Inbreuk op de persoonsgegevens binnen de vereiste termijn aan de bevoegde toezichthoudende autoriteit melden (overeenkomstig de Europese wetgeving inzake gegevensbescherming, onverwijld en, indien mogelijk, uiterlijk 72 uur nadat de inbreuk aan het licht is gekomen).

Betrokkenen zullen eveneens onverwijld op de hoogte worden gesteld in gevallen waarin de Inbreuk op de persoonsgegevens waarschijnlijk een hoog risico voor hun rechten en vrijheden met zich meebrengt, tenzij een dergelijke kennisgeving niet vereist is krachtens de Europese wetgeving inzake gegevensbescherming.

In overeenstemming met het bovenstaande worden Inbreuken op de persoonsgegevens waarvan Groepsleden het slachtoffer zijn geworden – met vermelding van de feiten, de gevolgen van dergelijke incidenten en de genomen corrigerende maatregelen – eveneens geregistreerd in Heracles, het register van de Santander Groep voor beveiligingsincidenten (waaronder Inbreuken op de persoonsgegevens), dat op verzoek ter beschikking zal worden gesteld aan de bevoegde toezichthoudende autoriteit.

Regel 4C – Groepsleden dienen ervoor te zorgen dat dienstverleners en andere entiteiten die namens hen persoonsgegevens verwerken, eveneens passende en gelijkwaardige beveiligingsmaatregelen treffen.

Groepsleden die gebruikmaken van een dienstverlener (die optreedt als verwerker) die toegang heeft tot de persoonsgegevens van betrokkenen (zoals een salarisadministrateur), dienen de verwerker schriftelijk contractuele verplichtingen op te leggen die voldoen aan de vereisten van de Europese wetgeving inzake gegevensbescherming, in de vorm van een bindende gegevensverwerkingsovereenkomst. Deze overeenkomst dient ten minste het volgende te bevatten:

- het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen;
- de verplichtingen en rechten van de verwerkingsverantwoordelijke;
- de volgende verplichtingen voor de entiteit die als verwerker optreedt:
    - De persoonsgegevens mogen uitsluitend worden verwerkt op basis van gedocumenteerde instructies van de verwerkingsverantwoordelijke, ook met betrekking tot doorgiften van persoonsgegevens naar een derde land of een internationale organisatie, tenzij de verwerker hiertoe verplicht is op grond van een wet waaraan hij onderworpen is (mits deze wet, voor zover van toepassing, voldoet aan de vereisten krachtens regel 13 hieronder). In een dergelijk geval dient de verwerker de verwerkingsverantwoordelijke vóór de verwerking in kennis te stellen van die wettelijke verplichting, tenzij die wet dergelijke informatie op grond van belangrijke redenen van algemeen belang verbiedt;
    - De verwerkingsverantwoordelijke dient ervoor te zorgen dat personen die bevoegd zijn om de persoonsgegevens te verwerken, zich tot geheimhouding hebben verplicht of onderworpen zijn aan een passende wettelijke geheimhoudingsplicht;
    - De verwerkingsverantwoordelijke dient passende technische en organisatorische maatregelen te nemen om een beveiligingsniveau te waarborgen dat in verhouding staat tot het risico dat de verwerking van de persoonsgegevens met zich meebrengt;

- Er mag geen andere verwerker worden ingeschakeld met betrekking tot de persoonsgegevens zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke en er dient, in voorkomend geval, een schriftelijke overeenkomst te worden gesloten met de verdere verwerker waarin dezelfde gegevensbeschermingsverplichtingen zijn vastgelegd als in de overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker (met name het bieden van voldoende waarborgen om passende technische en organisatorische maatregelen te treffen, zodat de verwerking voldoet aan de vereisten van de Europese wetgeving inzake gegevensbescherming);

- Er moet rekening worden gehouden met de aard van de verwerking en de verwerker moet de verwerkingsverantwoordelijke, voor zover mogelijk, bijstaan met passende technische en organisatorische maatregelen bij het nakomen van de verplichting van de verwerkingsverantwoordelijke om te reageren op verzoeken tot uitoefening van de rechten van de betrokkene (zoals nader beschreven in Regel 5 hieronder);

- De verwerker dient de verwerkingsverantwoordelijke te ondersteunen bij het waarborgen van de naleving van de verplichtingen met betrekking tot de implementatie van passende beveiligingsmaatregelen, het uitvoeren van gegevensbeschermingseffectbeoordelingen en de daarmee samenhangende raadplegingen van de bevoegde toezichthoudende autoriteiten; alsmede de meldingsplichten inzake Inbreuken op de persoonsgegevens aan de bevoegde toezichthoudende autoriteiten en de betrokkenen (indien van toepassing);

- Naar keuze van de verwerkingsverantwoordelijke dient de verwerker alle persoonsgegevens te verwijderen of aan de verwerkingsverantwoordelijke terug te geven na beëindiging van de dienstverlening met betrekking tot de verwerking, en bestaande kopieën te verwijderen, tenzij de opslag van de persoonsgegevens wettelijk verplicht is;

- De verwerkingsverantwoordelijke dient alle informatie ter beschikking te krijgen die nodig is om aan te tonen dat aan de verplichtingen als verwerker is voldaan, en om audits, met inbegrip van inspecties, die door de verwerkingsverantwoordelijke of een andere door de verwerkingsverantwoordelijke aangewezen auditor worden uitgevoerd, mogelijk te maken en daaraan mee te werken; en

- De verwerkingsverantwoordelijke dient onmiddellijk op de hoogte te worden gesteld indien een instructie naar de mening van de verwerker in strijd is met de wet.

REGEL 5 – EERBIEDIGING VAN DE RECHTEN VAN BETROKKENEN

Regel 5 – Groepsleden dienen verzoeken van betrokkenen met betrekking tot hun rechten op het gebied van gegevensbescherming te behandelen (waaronder verzoeken om inzage, rectificatie, verwijdering, beperking of overdracht van persoonsgegevens, bezwaren tegen de verwerking van persoonsgegevens, alsmede intrekking van toestemming).

Op verzoek zijn de betrokkenen gerechtigd om de volgende rechten uit te oefenen, zoals voorgeschreven door de Europese wetgeving inzake gegevensbescherming:

- Het recht op inzage, wat inhoudt dat informatie wordt verstrekt over de beschikbare persoonsgegevens van de betrokkene en dat wordt bevestigd of de persoonsgegevens van de betrokkene worden verwerkt;

- Het recht op rectificatie, op grond waarvan de betrokkene het recht heeft om rectificatie te verkrijgen van alle persoonsgegevens die mogelijk onjuist of onvolledig zijn;

- Het recht op verwijdering of het "recht om vergeten te worden", op grond waarvan de betrokkene het recht heeft om zijn of haar persoonsgegevens te laten verwijderen wanneer zich bepaalde omstandigheden voordoen (zoals bepaald in artikel 17 van de AVG);

- Het recht op beperking van de verwerking, op grond waarvan de betrokkene het recht heeft om de beperking van de verwerking van zijn of haar persoonsgegevens te verzoeken wanneer zich bepaalde omstandigheden voordoen (zoals bepaald in artikel 18 van de AVG);

- Het recht om elke ontvanger aan wie de persoonsgegevens zijn verstrekt, in kennis te stellen van elke rectificatie of verwijdering van persoonsgegevens of beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredige inspanningen vergt. De betrokkene kan ook verzoeken om geïnformeerd te worden over dergelijke ontvangers;

- Het recht op overdraagbaarheid van gegevens, op grond waarvan de betrokkene het recht heeft de hem of haar betreffende persoonsgegevens, die hij of zij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde vorm te ontvangen en die gegevens aan een andere verwerkingsverantwoordelijke over te dragen;

- Het recht van bezwaar, op grond waarvan de betrokkene het recht heeft bezwaar te maken tegen de verwerking van zijn of haar persoonsgegevens voor een specifiek doel, met inbegrip van verwerking ten behoeve van direct marketing en profilering voor zover die betrekking heeft op dergelijke marketing;

- Het recht om niet te worden onderworpen aan een besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking, met inbegrip van profilering, en dat rechtsgevolgen voor hem of haar heeft of hem of haar in aanzienlijke mate treft (indien van toepassing); en

- Het recht om de voor een specifieke verwerking gegeven toestemming te allen tijde in te trekken.

REGEL 6 – HET WAARBORGEN VAN ADEQUATE BESCHERMING BIJ DOORGIFTE EN VERDERE DOORGIFTE

Regel 6 – Groepsleden mogen geen persoonsgegevens doorgeven aan derden buiten Europa zonder te zorgen voor adequate bescherming van de persoonsgegevens, in overeenstemming met de normen die in dit Beleid zijn uiteengezet en in overeenstemming met de Europese wetgeving inzake gegevensbescherming.

Doorgifte en verdere doorgifte van persoonsgegevens door Groepsleden die onder de Europese wetgeving inzake gegevensbescherming vallen aan derden buiten Europa zijn niet toegestaan zonder dat hiervoor passende maatregelen worden genomen, zoals vereist door de Europese wetgeving inzake gegevensbescherming.

Deze maatregelen kunnen onder meer het volgende omvatten:

- het vaststellen dat de derde partij is gevestigd in een land waarvan de Europese Commissie heeft vastgesteld dat het een adequaat beschermingsniveau biedt voor de overgedragen persoonsgegevens; of

- het ondertekenen van passende modelcontractbepalingen of andere mechanismen waarin de Europese wetgeving inzake gegevensbescherming voorziet; of

- het waarborgen dat de doorgifte noodzakelijk is voor: (i) de uitvoering van een overeenkomst tussen de betrokkene en het doorgevende Groepslid of voor de uitvoering van precontractuele maatregelen die op verzoek van de betrokkene worden genomen; (ii) het sluiten of uitvoeren van een overeenkomst die in het belang van de betrokkene is gesloten tussen het doorgevende Groepslid en een andere partij; (iii) belangrijke redenen van algemeen belang die zijn erkend in het recht van de Unie of in het recht van de lidstaat waaraan de verwerkingsverantwoordelijke is onderworpen; (iv) het instellen, uitoefenen of verdedigen van rechtsvorderingen; (v) de bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon, wanneer de betrokkene niet in staat is toestemming te verlenen; of (vi) het verkrijgen van de uitdrukkelijke toestemming van betrokkenen, nadat deze betrokkenen zijn geïnformeerd over de mogelijke risico's van een dergelijke doorgifte als gevolg van het ontbreken van een adequaatheidsbesluit en passende waarborgen.

SECTIE B: PRAKTISCHE VERPLICHTINGEN

REGEL 7 – NALEVING EN VERANTWOORDING

Regel 7A – Groepsleden zijn verantwoordelijk voor de naleving van dit Beleid en moeten kunnen aantonen dat zij dit naleven; zij dienen te beschikken over geschikt personeel en de nodige ondersteuning om de naleving van dit Beleid binnen de gehele onderneming te waarborgen en daarop toe te zien.

De Santander Groep beschikt over een organisatorische structuur op het gebied van privacy die verantwoordelijk is voor het nemen van beslissingen, het coördineren, uitvoeren en controleren van alle activiteiten die binnen de Santander Groep plaatsvinden op het gebied van gegevensbescherming (het "**Privacyteam**"). De privacystructuur van de Santander Groep bestaat uit:

- **Corporate Data Protection Office** ("**Corporate DP Office**"): een bedrijfsorgaan dat verantwoordelijk is voor het vaststellen van de algemene criteria en het opstellen van het toepasselijke bedrijfsbeleid inzake gegevensbescherming. Samen met het team voor niet-financiële risico's vormt dit orgaan een wereldwijde tweede verdedigingslinie (2LoD, Second Line of Defense), die verantwoordelijk is voor het toezicht op het beheer van de privacygerelateerde activiteiten die door de eerste verdedigingslinie (1LoD, First Line of Defense) worden uitgevoerd, en voor het waarborgen van adequaat risicobeheer in overeenstemming met de risicobereidheid van de Santander Groep.

  Het Corporate DP Office en het team voor niet-financiële risico's nemen als wereldwijde 2LoD een reeks functies op zich voor alle entiteiten van de Santander Groep die onder de Europese wetgeving inzake gegevensbescherming vallen, waaronder met name:

  - Toezicht op naleving en controle: (i) toezicht houden op de naleving van de regels inzake gegevensbescherming binnen de Santander Groep; (ii) geconsolideerde rapportage aan het senior management van de Santander Groep; (iii) fungeren als wereldwijd aanspreekpunt, via de verschillende lokale functionarissen voor gegevensbescherming (FG's) (of soortgelijke functionarissen), bij de bevoegde toezichthoudende autoriteiten; (iv) het uitvoeren van impactanalyses, samen met de relevante bedrijfs- en ondersteunende functies, van beveiligingsincidenten op mondiaal niveau; (v) het uitvoeren van wereldwijde risicoanalyses en rapportages op het gebied van gegevensbescherming; en (vi) het faciliteren van bedrijfsbrede criteria en het fungeren als aanspreekpunt binnen de onderneming voor de FG's of Champions van de entiteiten (zie hieronder).

- Ondersteunende functie voor de FG's en Champions van de Santander Groep (organisatorische eenheden / entiteit(en) en lokale entiteiten). Dit houdt voornamelijk in dat gespecialiseerd advies wordt gegeven over regelgeving en ondersteuning wordt geboden bij de uitvoering van de lokale privacyfuncties.

- **Structuur en governance**

  - **Banco Santander (Corporation)**: twee sleutelfiguren ondersteunen het Corporate DP Office en rapporteren hieraan:

    - **De FG van Banco Santander** (officieel aangesteld bij de Spaanse toezichthoudende autoriteit): zijn of haar taken binnen de moedermaatschappij, die de FG op onafhankelijke wijze vervult, zijn beperkt tot de taken die in de AVG worden beschreven en die onder meer zijn of haar betrokkenheid vereisen bij het overleg met de Spaanse toezichthoudende autoriteit. Onverminderd de rapportage- en ondersteuningsverplichtingen van de FG ten opzichte van het Corporate DP Office, rapporteert de FG rechtstreeks aan het hoogste managementniveau van Banco Santander.

    - **Organisatorische eenheden**: eenheden die binnen de organisatie zijn aangesteld. Hun belangrijkste taken en verantwoordelijkheden bestaan uit: (a) het in eerste instantie afhandelen en oplossen van zaken met betrekking tot persoonsgegevens; (b) het informeren en adviseren van verwerkingsverantwoordelijken, verwerkers en werknemers over de wijze waarop aan de toepasselijke regelgeving inzake gegevensbescherming moet worden voldaan; (c) het toezicht houden op de naleving van de regelgeving inzake gegevensbescherming; (d) het fungeren als intern aanspreekpunt in de hoedanigheid van eerstelijnsondersteuning; (e) het doorsturen van vragen en verzoeken om ondersteuning naar het Corporate DP Office en het rapporteren van managementindicatoren.

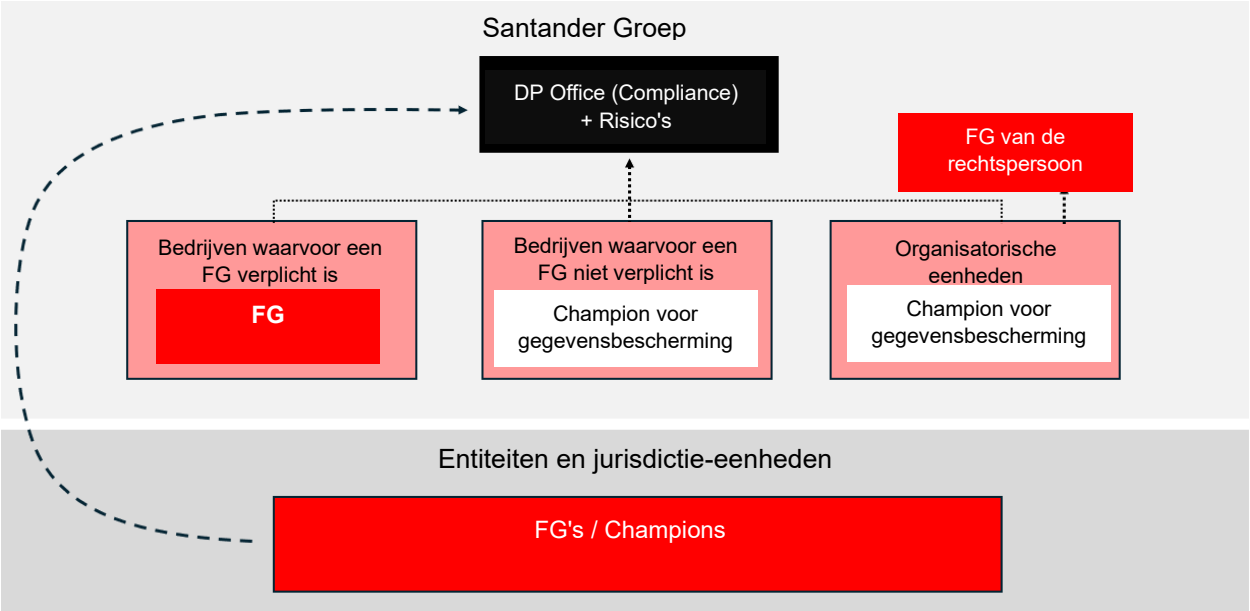
  - **Lokale eenheden**: er zijn ook twee functies die rapporteren aan het Corporate DP Office:

    - **FG's (of soortgelijke lokale functionarissen)**: indien vereist krachtens de Toepasselijke lokale wetgeving inzake gegevensbescherming wordt een FG (of soortgelijke lokale functionaris) aangesteld. Enkele van de belangrijkste taken en verantwoordelijkheden van een FG zijn: (a) fungeren als contactpersoon voor de betreffende toezichthoudende autoriteit en voor belanghebbenden; (b) samenwerking met de betreffende toezichthoudende autoriteit; (c) advies op het gebied van gegevensbescherming; (d) toezicht en controle; (e) training; (f) advies over gegevensbeschermingseffectbeoordelingen; (g) het voeren van voorafgaande raadplegingen met de betreffende toezichthoudende autoriteit; (h) toezicht op de registratie van verwerkingsactiviteiten; (i) advies over de melding van Inbreuken op de persoonsgegevens; (j) advies over het beheer van derden; en (k) toezicht op de uitoefening van de rechten van betrokkenen.

    - **Champions of soortgelijke lokale functionarissen (bijv. privacyfunctionarissen):**: wanneer er volgens de Toepasselijke lokale wetgeving inzake gegevensbescherming geen FG vereist is, of wanneer de omvang en/of complexiteit van een entiteit een groot aantal FG's of soortgelijke lokale functionarissen vereist, kunnen lokale Champions of

soortgelijke functionarissen (bijv. privacyfunctionarissen) het Corporate DP Office ondersteunen en hieraan rapporteren. De rol en verantwoordelijkheden van Champions komen sterk overeen met die van FG's of vergelijkbare functionarissen, met uitzondering van de communicatie met de toezichthoudende autoriteiten (waaraan zij niet deelnemen).

Hieronder vindt u een schema van de organisatiestructuur en de onderlinge relaties tussen de hierboven genoemde functionarissen die binnen de Santander Groep verantwoordelijk zijn voor gegevensbescherming:



Regel 7B – Groepsleden dienen passende technische en organisatorische maatregelen te treffen, zowel 'by design' als 'by default', om de naleving van het Beleid in de praktijk mogelijk te maken en te vergemakkelijken.

Rekening houdend met de stand van de techniek en de implementatiekosten, alsmede met de omvang, aard, context en doeleinden van de verwerking, zullen Groepsleden passende technische en organisatorische maatregelen treffen die voldoen aan de beginselen van gegevensbescherming 'by design' en 'by default', zoals vereist door de Europese wetgeving inzake gegevensbescherming. Groepsleden zullen dergelijke maatregelen in de verwerking integreren bij het vaststellen van de wijze van verwerking en het tijdstip van de verwerking zelf, teneinde de bescherming van de verwerkte persoonsgegevens te bevorderen en ervoor te zorgen dat standaard alleen die persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking.

Regel 7C – Groepsleden die persoonsgegevens verwerken dienen een schriftelijk register bij te houden (waaronder in elektronische vorm) van hun verwerkingsactiviteiten en dat register op verzoek ter beschikking te stellen aan de bevoegde toezichthoudende autoriteiten.

De registers van verwerkingsactiviteiten die worden bijgehouden door Groepsleden die optreden als verwerkingsverantwoordelijken, bevatten het volgende:

- de naam en contactgegevens van het Groepslid en, indien van toepassing, de gezamenlijke verwerkingsverantwoordelijke, de vertegenwoordiger van de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming;

- de doeleinden waarvoor persoonsgegevens worden verwerkt;

- een beschrijving van de categorieën betrokkenen van wie persoonsgegevens worden verwerkt en van de verwerkte persoonsgegevens;

- de categorieën ontvangers aan wie persoonsgegevens zijn of zullen worden verstrekt met inbegrip van ontvangers in derde landen of internationale organisaties;

- gegevens over het derde land of de derde landen waarnaar persoonsgegevens worden doorgegeven, met inbegrip van de identificatie van dat derde land of die internationale organisatie en de documentatie van passende waarborgen die zijn geïmplementeerd om dergelijke doorgiften te legitimeren (tenzij het land krachtens de Europese wetgeving inzake gegevensbescherming als adequaat is aangemerkt);

- voor zover mogelijk, de termijn gedurende welke de persoonsgegevens zullen worden bewaard; en

- voor zover mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die zijn getroffen om persoonsgegevens te beschermen.

De registers van verwerkingsactiviteiten die worden bijgehouden door Groepsleden die optreden als verwerkers voor een Groepslid dat de verwerkingsverantwoordelijke is, bevatten het volgende:

- de naam en contactgegevens van het Groepslid en van elke verwerkingsverantwoordelijke namens wie de verwerker optreedt, en, indien van toepassing, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker, en de functionaris voor gegevensbescherming;

- de categorieën verwerkingen die namens elke verwerkingsverantwoordelijke worden uitgevoerd;

- gegevens over het derde land of de derde landen waarnaar persoonsgegevens worden doorgegeven, waaronder de identificatie van dat derde land of die internationale organisatie en de documentatie van de passende waarborgen die zijn geïmplementeerd om dergelijke doorgiften te legitimeren (tenzij het land krachtens de Europese wetgeving inzake gegevensbescherming als adequaat is aangemerkt); en

- voor zover mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die zijn getroffen om persoonsgegevens te beschermen.

De registers van verwerkingsactiviteiten die worden bijgehouden door Groepsleden, dienen schriftelijk te zijn, waaronder in elektronische vorm, en worden op verzoek aan de bevoegde toezichthoudende autoriteiten beschikbaar gesteld.

REGEL 8 – TRAINING

Regel 8 – Groepsleden dienen passende training te bieden aan werknemers die permanente of regelmatige toegang hebben tot persoonsgegevens en/of die betrokken zijn bij de verwerking van persoonsgegevens of bij de ontwikkeling van hulpmiddelen die worden gebruikt om dergelijke persoonsgegevens te verwerken.

Groepsleden zullen passende en actuele training verzorgen voor werknemers die permanente of regelmatige toegang hebben tot persoonsgegevens en/of die betrokken zijn bij de verwerking van dergelijke persoonsgegevens of bij de ontwikkeling van hulpmiddelen die worden gebruikt om dergelijke persoonsgegevens te verwerken. Dergelijke training wordt ten minste eenmaal per twee jaar aangeboden en omvat onder meer procedures voor het behandelen van verzoeken van overheidsinstanties om toegang tot persoonsgegevens.

REGEL 9 – AUDIT

Regel 9 – Groepsleden dienen zich te houden aan het Auditprogramma zoals uiteengezet in Bijlage 1.

Groepsleden zullen zich houden aan het Auditprogramma door regelmatige interne audits uit te voeren en, waar nodig, externe audits toe te staan, in overeenstemming met het formele beoordelingsproces zoals vastgelegd in het Auditprogramma. De uitkomst van dergelijke audits zal worden gecommuniceerd in overeenstemming met Bijlage 1.

REGEL 10 – KLACHTENAFHANDELING

Regel 10 – Groepsleden dienen zich te houden aan de Procedure voor klachtenafhandeling zoals uiteengezet in Bijlage 2.

Groepsleden zullen zich houden aan de Procedure voor klachtenafhandeling zoals uiteengezet in Bijlage 2 om klachten van betrokkenen op adequate wijze af te handelen en de verwerking van persoonsgegevens door Groepsleden te waarborgen. Groepsleden zullen tevens de uitoefening van de rechten van derde-begunstigden zoals uiteengezet in sectie C van dit Beleid mogelijk maken.

REGEL 11 – SAMENWERKING MET BEVOEGDE TOEZICHTHOUDENDE AUTORITEITEN

Regel 11 – Groepsleden dienen zich te houden aan de Samenwerkingsprocedure zoals uiteengezet in Bijlage 3.

Groepsleden zullen zich houden aan de Samenwerkingsprocedure zoals uiteengezet in Bijlage 3 en zullen met de bevoegde toezichthoudende autoriteiten samenwerken, zich laten controleren en inspecteren door deze autoriteiten (waar nodig ook ter plaatse) met betrekking tot dit Beleid; tevens zullen zij hun advies in overweging nemen en zich houden aan hun beslissingen inzake alle aangelegenheden die verband houden met dit Beleid.

REGEL 12 – ACTUALISERING VAN DE REGELS

Regel 12 – Groepsleden dienen zich te houden aan de Actualiseringsprocedure zoals uiteengezet in Bijlage 4.

Groepsleden zullen zich houden aan de Actualiseringsprocedure zoals uiteengezet in Bijlage 4 en zullen elke wijziging van dit Beleid en de lijst van Groepsleden onverwijld meedelen aan de bevoegde toezichthoudende autoriteiten, de betrokkenen en de Groepsleden, voor zover nodig.

REGEL 13 – MAATREGELEN INDIEN NATIONALE WETGEVING DE NALEVING VAN HET BELEID VERHINDERT

Regel 13A – Groepsleden verbinden zich ertoe dit Beleid uitsluitend te gebruiken als instrument voor doorgiften aan Importerende entiteiten wanneer zij zorgvuldig hebben beoordeeld dat de wetgeving en praktijken in het land van de Importerende entiteiten (met inbegrip van eventuele vereisten tot openbaarmaking van persoonsgegevens of maatregelen die overheidsinstanties toegang verlenen) hen niet beletten hun verplichtingen uit hoofde van dit Beleid na te komen.

Groepsleden zullen dit Beleid alleen gebruiken als instrument om internationale doorgiften te waarborgen wanneer zij hebben vastgesteld dat de wetgeving en praktijken in de betreffende derde landen van bestemming, met inbegrip van eventuele vereisten tot openbaarmaking van persoonsgegevens of maatregelen die overheidsinstanties toegang verlenen, hen niet beletten hun verplichtingen uit hoofde van dit Beleid na te komen. Dit berust op de opvatting dat wetgeving en praktijken die de essentie van de fundamentele rechten en vrijheden eerbiedigen en niet verder gaan dan wat in een democratische samenleving noodzakelijk en evenredig is, niet in strijd zijn met het Beleid.

Bij de beoordeling van de wetgeving en praktijken van de derde landen die van invloed kunnen zijn op de naleving van de in dit Beleid opgenomen verplichtingen, zullen de Groepsleden met name aandacht besteden aan de volgende elementen:

(i) de specifieke omstandigheden van de doorgifte of reeks doorgiften, en van eventuele voorgenomen verdere doorgiften binnen hetzelfde derde land of naar een ander derde land, met inbegrip van:

- de doeleinden waarvoor de gegevens worden doorgegeven en verwerkt (zoals marketing, HR, opslag, IT-ondersteuning enz.);
- de soorten entiteiten die bij de verwerking betrokken zijn (de Importerende entiteit en eventuele verdere ontvangers bij verdere doorgifte);
- de economische sector waarin de doorgifte of reeks doorgiften plaatsvindt;
- de categorieën en de vorm van doorgegeven persoonsgegevens;
- de locatie van de verwerking, met inbegrip van opslag; en
- de gebruikte transmissiekanalen.

(ii) de wetgeving en praktijken van de derde landen van bestemming die relevant zijn in het licht van de omstandigheden van de doorgifte. Deze kunnen het volgende omvatten: (a) wetgeving en praktijken die de openbaarmaking van gegevens aan overheidsinstanties voorschrijven of toegang door dergelijke instanties toestaan; (b) wetgeving en praktijken die voorzien in toegang tot deze gegevens tijdens de doorgifte tussen de landen van de Exporterende entiteiten en de landen van de Importerende entiteiten; en (c) de toepasselijke beperkingen en waarborgen.

(iii) alle relevante contractuele, technische of organisatorische waarborgen die zijn ingesteld ter aanvulling van de waarborgen krachtens dit Beleid. Dit omvat maatregelen die worden toegepast tijdens de doorgifte en bij de verwerking van de persoonsgegevens in de landen van bestemming.

Indien er aanvullende waarborgen moeten worden ingesteld naast de waarborgen waarin dit Beleid voorziet, dienen het Aansprakelijke BCR-lid en de betreffende FG of de Champion, al naar gelang het geval, hiervan op de hoogte te worden gesteld en bij de beoordeling te worden betrokken. Groepsleden dienen deze beoordeling,

evenals de gekozen en geïmplementeerde aanvullende maatregelen, op passende wijze te documenteren. Zij dienen deze documentatie op verzoek ter beschikking te stellen aan de bevoegde toezichthoudende autoriteit.

Importerende entiteiten dienen Exporterende entiteiten onverwijld in kennis te stellen indien zij, bij het gebruik van dit Beleid als instrument voor doorgiften en gedurende de looptijd van het lidmaatschap, redenen hebben om aan te nemen dat zij onderworpen zijn of zijn geworden aan wetgeving of praktijken die hen zouden beletten hun verplichtingen krachtens dit Beleid na te komen. Dit omvat onder meer het onvermogen om aan hun verplichtingen te voldoen als gevolg van een wetswijziging in het betreffende derde land of een maatregel (zoals een verzoek tot openbaarmaking). Deze informatie dient tevens te worden verstrekt aan het Aansprakelijke BCR-lid.

Na verificatie van een dergelijke melding verbinden de betrokken Exporterende entiteit, samen met het Aansprakelijke BCR-lid en, al naar gelang het geval, de betreffende FG of Champion, zich ertoe onverwijld aanvullende maatregelen vast te stellen (zoals technische of organisatorische maatregelen ter waarborging van de veiligheid en vertrouwelijkheid), die door de Exporterende entiteit en/of de Importerende entiteit moeten worden genomen, teneinde hen in staat te stellen aan hun verplichtingen krachtens dit Beleid te voldoen. Hetzelfde geldt indien een Exporterende entiteit redenen heeft om aan te nemen dat een Importerende entiteit haar verplichtingen krachtens dit Beleid niet langer kan nakomen.

Wanneer de relevante Exporterende entiteit, samen met het Aansprakelijke BCR-lid en de betreffende FG of Champion, al naar gelang het geval, vaststelt dat het Beleid – zelfs indien vergezeld van aanvullende maatregelen – niet kan worden nageleefd voor een doorgifte of een reeks doorgiften, of indien zij hiertoe instructies ontvangt van de bevoegde toezichthoudende autoriteit, verbindt zij zich ertoe de betreffende doorgifte of reeks doorgiften op te schorten, evenals alle doorgiften waarvoor dezelfde beoordeling en redenering tot een soortgelijk resultaat zouden leiden, totdat de naleving opnieuw is gewaarborgd of de doorgifte is beëindigd.

Na een dergelijke opschorting dient de Exporterende entiteit de doorgifte of reeks doorgiften te beëindigen indien dit Beleid niet kan worden nageleefd en de naleving niet binnen één maand na de opschorting is hersteld. In dit geval dienen persoonsgegevens die vóór de opschorting zijn doorgegeven, alsmede eventuele kopieën daarvan, naar keuze van de Exporterende entiteit in hun geheel te worden teruggegeven of vernietigd.

Het Aansprakelijke BCR-lid en de betreffende FG of Champion, al naar gelang het geval, zullen alle andere Groepsleden op de hoogte stellen van de uitgevoerde beoordeling en de resultaten daarvan, zodat de vastgestelde aanvullende maatregelen worden toegepast indien hetzelfde type doorgiften door een ander Groepslid wordt uitgevoerd of – indien er geen doeltreffende aanvullende maatregelen konden worden getroffen – de betreffende doorgiften worden opgeschort of beëindigd.

Exporterende entiteiten dienen tevens voortdurend, en waar van toepassing in samenwerking met Importerende entiteiten, toezicht te houden op ontwikkelingen in de derde landen waarnaar Exporterende entiteiten persoonsgegevens hebben doorgegeven, die van invloed kunnen zijn op de oorspronkelijke beoordeling van het beschermingsniveau en de op basis daarvan genomen besluiten inzake dergelijke doorgiften.

Regel 13B – Importerende entiteiten dienen ervoor te zorgen dat, wanneer zij van een overheidsinstantie een juridisch bindend verzoek ontvangen op grond van de wetgeving van het land van bestemming tot openbaarmaking van persoonsgegevens die overeenkomstig het Beleid zijn doorgegeven, of wanneer zij kennis nemen van enige directe toegang door overheidsinstanties tot persoonsgegevens die overeenkomstig het Beleid zijn doorgegeven in overeenstemming met de wetgeving van het land van bestemming, zij dan de Exporterende entiteit onverwijld hiervan in kennis stellen en, indien mogelijk, de betrokkene (indien nodig met hulp van de Exporterende entiteit).

Importerende entiteiten zullen de betreffende Exporterende entiteit onverwijld in kennis stellen en, indien mogelijk, de betrokkene (indien nodig met hulp van de Exporterende entiteit) indien zij:

- een juridisch bindend verzoek ontvangen van een overheidsinstantie krachtens de wetgeving van het land van bestemming of een ander derde land, tot openbaarmaking van persoonsgegevens die overeenkomstig het Beleid zijn doorgegeven (een dergelijke kennisgeving dient informatie te bevatten over de opgevraagde persoonsgegevens, de verzoekende instantie, de rechtsgrondslag voor het verzoek en het gegeven antwoord); of

- kennis nemen van enige directe toegang door overheidsinstanties tot persoonsgegevens die overeenkomstig het Beleid zijn doorgegeven in overeenstemming met de wetgeving van het land van bestemming (een dergelijke kennisgeving dient alle informatie te bevatten waarover de Importerende entiteit beschikt).

Indien het de Importerende entiteit verboden is de Exporterende entiteit en/of de betrokkene in kennis te stellen van de toegang tot de gegevens, zal de Importerende entiteit zich naar beste vermogen inspannen om ontheffing van dit verbod te verkrijgen, teneinde de Exporterende entiteit zo spoedig mogelijk zoveel mogelijk informatie te verstrekken, en zal zij deze inspanningen documenteren om deze op verzoek van de Exporterende entiteit te kunnen aantonen.

De Importerende entiteit zal de Exporterende entiteit met regelmatige tussenpozen zoveel mogelijk relevante informatie verstrekken over de ontvangen verzoeken (met name het aantal verzoeken, het soort gevraagde gegevens, de verzoekende autoriteit(en), of er bezwaar is gemaakt tegen verzoeken en de uitkomst van dergelijke bezwaren enz. Indien het de Importerende entiteit geheel of gedeeltelijk verboden is of wordt om de Exporterende entiteit de bovengenoemde informatie te verstrekken, dient zij de Exporterende entiteit hiervan onverwijld op de hoogte te stellen.

De Importerende entiteit bewaart de bovengenoemde informatie zolang de gegevens onderworpen zijn aan de waarborgen waarin het Beleid voorziet en stelt deze op verzoek ter beschikking aan de bevoegde toezichthoudende autoriteit.

De Importerende entiteit zal de rechtmatigheid van het verzoek tot openbaarmaking toetsen, met name of dit binnen de bevoegdheden valt die aan de verzoekende overheidsinstantie zijn toegekend, en zal het verzoek aanvechten indien zij na zorgvuldige beoordeling tot de conclusie komt dat er redelijke gronden zijn om aan te nemen dat het verzoek onrechtmatig is krachtens de wetgeving van het land van bestemming, de toepasselijke verplichtingen krachtens het internationaal recht en de beginselen van internationale hoffelijkheid. De Importerende entiteit zal, onder dezelfde voorwaarden, de mogelijkheden tot beroep benutten. Bij het aanvechten van een verzoek zal de Importerende entiteit om voorlopige maatregelen verzoeken teneinde de gevolgen van het verzoek op te schorten totdat de bevoegde gerechtelijke autoriteit een uitspraak heeft gedaan over de gegrondheid ervan. Zij zal de gevraagde persoonsgegevens niet openbaar maken totdat zij daartoe krachtens de toepasselijke procedureregels verplicht is.

De Importerende entiteit zal haar juridische beoordeling en eventuele betwisting van het verzoek tot openbaarmaking documenteren en, voor zover toegestaan krachtens de wetgeving van het land van bestemming, deze documentatie ter beschikking stellen aan de Exporterende entiteit. Zij zal deze documentatie op verzoek ook ter beschikking stellen aan de bevoegde toezichthoudende autoriteit.

De Importerende entiteit verstrekt bij het beantwoorden van een verzoek tot openbaarmaking de minimaal toegestane hoeveelheid informatie, op basis van een redelijke interpretatie van het verzoek.

In ieder geval zullen de Groepsleden ervoor zorgen dat eventuele doorgiften van persoonsgegevens krachtens dit Beleid aan een overheidsinstantie niet massaal, onevenredig of willekeurig zijn op een wijze die verder gaat dan wat in een democratische samenleving noodzakelijk is.

REGEL 14 – NIET-NALEVING VAN HET BELEID EN BEËINDIGING

Regel 14A – Exporterende entiteiten mogen persoonsgegevens uitsluitend doorgeven aan Importerende entiteiten die daadwerkelijk aan het Beleid gebonden zijn en aan de nalevingsvereisten kunnen voldoen.

Er vindt krachtens dit Beleid geen doorgifte plaats aan een Groepslid, tenzij dit Groepslid daadwerkelijk aan het Beleid gebonden is en aan de nalevingsvereisten kan voldoen. Wanneer een Importerende entiteit om welke reden dan ook niet aan het Beleid kan voldoen, dient zij de Exporterende entiteit hiervan onverwijld op de hoogte te stellen. Indien de Importerende entiteit het Beleid schendt of niet aan het Beleid kan voldoen, zal de Exporterende entiteit de doorgifte opschorten of niet uitvoeren.

De Importerende entiteit dient, naar keuze van de Exporterende entiteit, de persoonsgegevens die krachtens het Beleid zijn doorgegeven, onmiddellijk in hun geheel terug te geven of te verwijderen indien:

- de Exporterende entiteit de doorgifte heeft opgeschort en de naleving van dit Beleid niet binnen een redelijke termijn, en in elk geval niet binnen één maand na de opschorting, is hersteld; of
- de Importerende entiteit het Beleid op substantiële of aanhoudende wijze schendt; of
- de Importerende entiteit zich niet houdt aan een bindende uitspraak van een bevoegde rechtbank of bevoegde toezichthoudende autoriteit met betrekking tot haar verplichtingen krachtens het Beleid.

Hetzelfde geldt voor eventuele kopieën van de gegevens. De Importerende entiteit dient de verwijdering van de gegevens aan de Exporterende entiteit te bevestigen. Zolang de gegevens niet zijn verwijderd of teruggegeven, dient de Importerende entiteit te blijven zorgen voor naleving van het Beleid. Indien er een wettelijk verbod bestaat voor de Importerende entiteit om de doorgegeven persoonsgegevens terug te geven of te verwijderen, garandeert de Importerende entiteit dat zij zich zal blijven houden aan het Beleid en de gegevens slechts zal verwerken voor zover en zolang dit wettelijk vereist is.

Regel 14B – Een Importerende entiteit die niet langer aan het Beleid gebonden is, dient ervoor te zorgen dat persoonsgegevens op passende wijze worden bewaard, teruggegeven of verwijderd, al naar gelang het geval.

Een Importerende entiteit die niet langer aan het Beleid gebonden is, mag de krachtens dit Beleid ontvangen persoonsgegevens, al naar gelang het geval, bewaren, teruggeven of verwijderen. Indien de Exporterende en de Importerende entiteit overeenkomen dat de gegevens door de Importerende entiteit mogen worden bewaard, moet de bescherming krachtens dit Beleid worden gehandhaafd.

SECTIE C: RECHTEN VAN DERDE-BEGUNSTIGDEN

C.1 Betrokkenen van wie de persoonsgegevens aan een Importerende entiteit worden doorgegeven, moeten als derde-begunstigden bepaalde rechten kunnen uitoefenen. Daartoe kunnen betrokkenen de naleving afdwingen van:

- regels 1B en 1C van het Beleid (betreffende eerlijkheid en rechtmatigheid, en de verwerking van bijzondere categorieën persoonsgegevens);

- regel 2 van het Beleid (betreffende transparantie en de verwerking van persoonsgegevens uitsluitend voor een bekend doel);

- regel 3 van het Beleid (betreffende gegevensminimalisatie, nauwkeurigheid en beperkte bewaartermijnen);

- regel 4 van het Beleid (betreffende passende beveiligingsmaatregelen en verplichtingen inzake melding van inbreuken op de gegevensbeveiliging);

- regel 5 van het Beleid (betreffende het eerbiedigen van de rechten van betrokkenen);

- regel 6 van het Beleid (betreffende adequate bescherming bij doorgiften en verdere doorgiften);

- regel 10 van het Beleid (betreffende klachtenafhandeling);

- regel 11 van het Beleid (betreffende samenwerking met bevoegde toezichthoudende autoriteiten);

- regel 12 van het Beleid (betreffende de actualisering van de regels);

- regel 13 van het Beleid (betreffende maatregelen indien nationale wetgeving de naleving van het Beleid verhindert);

- de bepalingen in C1 tot en met C3, waarin rechten aan derden als begunstigden worden toegekend en waarin de aansprakelijkheids- en bevoegdheidsregels in het kader van het Beleid worden vastgelegd; en

- het recht op inzage in het Beleid dat beschikbaar is op de online webpagina, op het interne netwerk (toegankelijk voor werknemers) van het bedrijf of het recht om een papieren exemplaar van het Beleid te verkrijgen, evenals een lijst van Groepsleden die aan dit Beleid gebonden zijn.

door:

- *een klacht in te dienen*: betrokkenen kunnen klachten indienen bij een Groepslid (overeenkomstig de in Bijlage 2 uiteengezette Procedure voor klachtenafhandeling) en bij de toezichthoudende autoriteit in de Lidstaat waar de vermeende inbreuk heeft plaatsgevonden, of waar de betrokkene gewoonlijk werkt of verblijft; en/of

- *een procedure aan te spannen*: betrokkenen kunnen een procedure aanspannen tegen Groepsleden bij de rechtbanken van een Lidstaat waar het Groepslid een vestiging heeft, of in de Lidstaat waar de betrokkene zijn gewone verblijfplaats heeft.

Zoals nader wordt toegelicht in de secties C.2 tot en met C.4, behouden betrokkenen, wanneer een inbreuk wordt begaan door een Groepslid dat buiten de EER is gevestigd, het recht om klachten in te dienen bij en een procedure aan te spannen tegen het aangewezen Aansprakelijke BCR-lid, als ware de inbreuk begaan door die entiteit in de Lidstaat waar deze is gevestigd.

Deze rechten hebben geen betrekking op die onderdelen van het Beleid die betrekking hebben op interne mechanismen die binnen Groepsleden zijn geïmplementeerd, zoals details over training, het auditprogramma, het compliance-netwerk en het mechanisme voor de actualisering daarvan.

Bovendien aanvaarden Groepsleden dat betrokkenen kunnen worden vertegenwoordigd door een instelling, organisatie of vereniging zonder winstoogmerk onder de voorwaarden zoals uiteengezet in artikel 80, lid 1, van de AVG.

C.2 Betrokkenen kunnen tevens passende rechtsmiddelen inroepen bij het Aansprakelijke BCR-lid, dat ermee instemt de nodige maatregelen te nemen om elke inbreuk op de in subsectie C.1 genoemde bepalingen door een Importerende entiteit te verhelpen en, indien van toepassing, schadevergoeding te ontvangen van het Aansprakelijke BCR-lid voor alle schade (hetzij materieel, hetzij immaterieel) die is geleden als gevolg van een inbreuk op de bepalingen of een van de bepalingen vermeld in subsectie C.1 door een Importerende entiteit, overeenkomstig de uitspraak van een rechtbank of andere bevoegde autoriteit.

C.3 Teneinde elke twijfel weg te nemen, genieten betrokkenen de rechten van derde-begunstigden zoals beschreven in deze sectie C, en zijn de Europese rechtbanken of bevoegde toezichthoudende autoriteiten bevoegd als ware de schending van de in deze sectie C beschreven bepalingen of een daarvan veroorzaakt door het Aansprakelijke BCR-lid.

C.4 In het geval dat een vordering wordt ingediend vanwege schade die een betrokkene heeft geleden als gevolg van een inbreuk op dit Beleid, zijn de Groepsleden overeengekomen dat de bewijslast om aan te tonen dat een Importerende entiteit niet verantwoordelijk is voor de inbreuk, of dat er geen sprake was van een dergelijke inbreuk, berust bij het Aansprakelijke BCR-lid.

DEEL III: BIJLAGEN

BIJLAGE 1

AUDITPROGRAMMA

1. INLEIDING

1.1 Groepsleden moeten controleren of ze zich aan het Beleid houden en moeten daarbij aan bepaalde voorwaarden voldoen. In dit document staat hoe Groepsleden met die vereisten omgaan.

1.2 Tot de *dagelijkse werkzaamheden* (BAU, business as usual)hoort het geven van advies over de verwerking van persoonsgegevens die onder dit Beleid vallen, en het beoordelen van de verwerking van persoonsgegevens door Groepsleden op mogelijke privacygerelateerde risico's in de dagelijkse bedrijfsvoering. De verwerking van persoonsgegevens wordt daarom voortdurend grondig gecontroleerd en geëvalueerd.

1.3 Als wereldwijde tweede verdedigingslinie (2LoD) neemt het Corporate DP Office de monitoring en controle op zich, inclusief het toezicht op de naleving van de gegevensbeschermingsregels binnen de Santander Groep.

1.4 Anderzijds bestaat het Auditprogramma uit de formele, onafhankelijke beoordeling die wordt uitgevoerd door de derde verdedigingslinie (3LoD) om naleving van het Beleid te waarborgen, zoals vereist door de bevoegde toezichthoudende autoriteiten. Het oordeel van de auditafdeling (3LoD) is een onafhankelijk oordeel en vervangt niet de controle- en toezichtverantwoordelijkheden van de eerste en tweede verdedigingslinie (1LoD en 2LoD), die ook deel uitmaken van de reikwijdte van de audit bij het beoordelen van de verankering en implementatie van dit Beleid.

2. AANPAK

2.1 <u>Overzicht van de audit</u>

Wie er verantwoordelijk is voor het uitvoeren van de audits om te controleren of het Beleid wordt nageleefd en ervoor te zorgen dat deze audits alle aspecten van het Beleid bestrijken, kan per Groepslid verschillen, afhankelijk van de specifieke omstandigheden. Meestal worden audits uitgevoerd onder toezicht van interne of externe erkende auditors (afhankelijk van de situatie), die gegarandeerd onafhankelijk zijn bij het uitvoeren van hun taken met betrekking tot deze audits. De betreffende auditor zorgt ervoor dat eventuele problemen of gevallen van niet-naleving onder de aandacht van het hogere management worden gebracht en dat eventuele corrigerende maatregelen om naleving te waarborgen, binnen een redelijke termijn worden genomen.

2.2 <u>Moment en reikwijdte van de audit</u>

2.2.1 De afdeling Interne audit bepaalt, in overeenstemming met haar risicobeoordelingsmethodiek, het moment van de audits binnen een maximale auditcyclus van 4 jaar.

Niettemin zullen de eerste audits plaatsvinden binnen de eerste 24 maanden nadat het Beleid formeel is goedgekeurd en dus van kracht is geworden. Daarna wordt de audit uitgevoerd volgens de toepasselijke risicogebaseerde auditmethodiek, zoals aangegeven in de eerste alinea van deze sectie 2.2.

Groepsleden moeten altijd een audit uitvoeren als (i) er aanwijzingen zijn dat dit Beleid niet wordt nageleefd; of (ii) het Privacyteam om een specifieke (ad-hoc) audit vraagt.

2.2.2 In lijn hiermee worden de reikwijdte en het toepassingsgebied van de audit bepaald door de afdeling Interne Audit op basis van een risicoanalyse volgens de goedgekeurde methodiek.

2.2.3 Alle aspecten van dit Beleid (bijv. applicaties, IT-systemen, doorgifte van gegevens enz.), inclusief methoden en actieplannen die ervoor zorgen dat corrigerende maatregelen zijn doorgevoerd, worden beoordeeld volgens een op risico's gebaseerde aanpak om de specifieke reikwijdte van de audit te bepalen. Dit gebeurt, zoals hierboven beschreven, met regelmatige tussenpozen.

2.3 Auditors

2.3.1 De audits in het kader van dit programma worden uitgevoerd door interne auditors van de afdeling Interne Audit of door externe erkende auditors, al naar gelang het geval. Wanneer audits worden uitgevoerd door externe auditors, dient aan de volgende voorwaarden te worden voldaan:

(a) Voer voorafgaand aan de selectie een gedegen due diligence-onderzoek uit om te waarborgen dat de betreffende auditors over de juiste kwalificaties en status beschikken om bij deze werkzaamheden te kunnen assisteren; en

(b) Sluit een overeenkomst met deze auditors om de levering van hun diensten te waarborgen in overeenstemming met de toepasselijke regelgeving.

2.4 Onafhankelijkheid

2.4.1 Voor personen die verantwoordelijk zijn voor het vaststellen van het auditprogramma of het uitvoeren van de audits, is onafhankelijkheid bij de uitoefening van hun taken gewaarborgd.

2.5 Verslag

2.5.1 Na afronding van de audit worden, afhankelijk van de aard ervan, het verslag en de bevindingen ter beschikking gesteld aan het hogere management, het Corporate DP Office, de betreffende FG of Champion, en wordt hiervan melding gemaakt bij de Auditcommissie van de Raad van Bestuur en aan de Raad van Bestuur van het Aansprakelijke BCR-lid. Het auditverslag bevat tevens details over eventuele vereiste corrigerende maatregelen, aanbevelingen en tijdschema's voor de uitvoering van deze maatregelen.

2.5.2 De Groepsleden zijn overeengekomen om op verzoek kopieën van de resultaten van elke audit van het Beleid te verstrekken aan elke bevoegde toezichthoudende autoriteit.

2.5.3 De betreffende FG of Champion is verantwoordelijk voor het onderhouden van contacten met de bevoegde toezichthoudende autoriteiten ten behoeve van het verstrekken van de hierboven beschreven informatie.

BIJLAGE 2

PROCEDURE VOOR KLACHTENAFHANDELING

1. INLEIDING

1.1 Het doel van deze Procedure voor klachtenafhandeling is toe te lichten hoe klachten worden afgehandeld die worden ingediend door een betrokkene van wie de persoonsgegevens door Groepsleden krachtens het Beleid worden verwerkt.

2. HOE BETROKKENEN EEN KLACHT KUNNEN INDIENEN

Alle klachten van betrokkenen van wie de persoonsgegevens worden verwerkt overeenkomstig dit Beleid, kunnen schriftelijk (ook per e-mail) worden ingediend bij de betreffende FG of Champion, al naar gelang het geval. Betrokkenen kunnen een klacht indienen via de volgende contactgegevens:

Ter attentie van: Privacyteam

Adres: vul een postadres in

E-mailadres: Een lijst met de relevante e-mailadressen vindt u hier.

Indien klachten via andere kanalen worden ingediend, zullen deze in ieder geval eveneens in behandeling worden genomen, mits het betreffende Groepslid hiervan naar behoren in kennis wordt gesteld.

3. DOOR WIE WORDEN KLACHTEN AFGEHANDELD?

3.1 De betreffende FG of Champion, al naar gelang het geval, handelt alle klachten af die in het kader van dit Beleid worden ingediend met betrekking tot de verwerking van persoonsgegevens. De FG of de verantwoordelijke, al naar gelang het geval, zal contact opnemen met de betrokken bedrijfsonderdelen om de klacht te onderzoeken en zal de afhandeling coördineren (waarbij onder meer informatie aan de klager wordt verstrekt over de genomen maatregelen).

3.2 Wat is de reactietermijn?

De FG of Champion zal, met ondersteuning van het Privacyteam, binnen tien werkdagen de ontvangst van een klacht aan de betrokken persoon bevestigen, de klacht onderzoeken en vervolgens een inhoudelijk antwoord geven door informatie te verstrekken over de genomen maatregelen, zonder onnodige vertraging en in ieder geval binnen één kalendermaand. Indien, vanwege de complexiteit van de klacht of het aantal verzoeken, binnen deze termijn geen inhoudelijk antwoord kan worden gegeven, zal de FG of de Champion, met ondersteuning van het Privacyteam, de klager binnen één kalendermaand na ontvangst van de klacht op de hoogte stellen van de redenen voor de vertraging en een redelijke geschatte termijn (van maximaal twee extra kalendermaanden vanaf de datum waarop de betrokkene op de hoogte is gesteld van de verlenging) voor het antwoord aangeven.

Indien de reactietermijn niet wordt gehaald en het antwoord op de klacht zonder gemotiveerde reden wordt uitgesteld, kan de betrokkene dit melden aan de FG of de Champion, die dan zonder onnodige vertraging en in ieder geval binnen tien kalenderdagen de redenen voor deze vertraging zal toelichten en de betrokkene zal informeren over de tot dusver genomen maatregelen. De zaak zal worden

doorverwezen naar het Corporate DP Office (vergezeld van een met redenen omkleed rapport waarin de te nemen maatregelen worden vastgesteld), dat de zaak zal beoordelen en de FG of de Champion zal adviseren over de wijze waarop de in de klacht aan de orde gestelde kwesties zo spoedig mogelijk kunnen worden opgelost. In ieder geval kan de betrokkene ook gebruikmaken van de rechten zoals beschreven in sectie 3.4 van deze Bijlage 2.

3.3 Wanneer een klager bezwaar maakt tegen een bevinding of de afwijzing van een klacht

Indien een klacht als gegrond wordt beschouwd, zal de FG of de Champion de nodige maatregelen nemen om de door de betrokkene aan de orde gestelde kwestie op te lossen en hem of haar hiervan op de hoogte stellen.

Indien de klager bezwaar maakt tegen het antwoord van de FG of de Champion (ook indien dit antwoord een weigering inhoudt om de klacht in behandeling te nemen of hieraan gevolg te geven) of tegen enig aspect van een bevinding, kan hij of zij de betreffende FG of Champion hiervan op de hoogte stellen. De zaak zal worden doorverwezen naar het Corporate DP Office dat de zaak zal beoordelen en, via de FG of Champion van de entiteit, de klager zal informeren over de definitieve beslissing om de oorspronkelijke bevinding te aanvaarden of deze te vervangen door een nieuwe bevinding. Het betreffende lokale DP Office zal de klager binnen één kalendermaand na de doorverwijzing antwoorden. Indien, vanwege de complexiteit van de klacht, binnen deze termijn geen inhoudelijk antwoord kan worden gegeven, zal het Corporate DP Office de klager binnen één kalendermaand na ontvangst van de doorverwijzing op de hoogte stellen van de reden voor de vertraging en een redelijke geschatte termijn (van maximaal twee extra kalendermaanden) voor het antwoord aangeven. Indien de klacht gegrond wordt verklaard, zal het Corporate DP Office ervoor zorgen dat de nodige maatregelen als gevolg daarvan worden genomen.

3.4 Alternatieve klachtenmechanismen

Betrokkenen van wie de persoonsgegevens overeenkomstig dit Beleid worden verwerkt, hebben tevens het recht om: (i) een klacht in te dienen bij de toezichthoudende autoriteit in de Lidstaat waar de vermeende inbreuk heeft plaatsgevonden, of waar de betrokkene gewoonlijk werkt of verblijft; en/of (ii) een claim in te dienen bij een bevoegde rechtbank in het Europese land waar het Groepslid is gevestigd of in het Europese land waar de betrokkene verblijft. Zoals nader wordt toegelicht in de secties C.2 tot en met C.4, behouden betrokkenen, wanneer een inbreuk wordt begaan door een Groepslid dat buiten de EER is gevestigd, het recht om klachten in te dienen bij en een procedure aan te spannen tegen het aangewezen Aansprakelijke BCR-lid, als ware de inbreuk begaan door die entiteit in de Lidstaat waar deze is gevestigd. Deze rechten zijn van toepassing, ongeacht of de betrokkenen eerst een klacht hebben ingediend bij een Groepslid via deze Procedure voor klachtenafhandeling.

BIJLAGE 3

SAMENWERKINGSPROCEDURE

1. SAMENWERKINGSPROCEDURE

1.1 In deze Samenwerkingsprocedure wordt uiteengezet op welke wijze Groepsleden zullen samenwerken met de bevoegde toezichthoudende autoriteiten en zich zullen onderwerpen aan controles en inspecties door deze autoriteiten (waar nodig ook ter plaatse) met betrekking tot dit Beleid; tevens wordt hierin vastgelegd dat zij het advies van deze autoriteiten in overweging zullen nemen en zich zullen houden aan hun beslissingen inzake alle aangelegenheden die verband houden met dit Beleid..

1.2 Indien nodig zullen de Groepsleden het benodigde personeel ter beschikking stellen voor overleg met de bevoegde toezichthoudende autoriteit met betrekking tot het Beleid.

1.3 Op verzoek zal de betreffende FG of Champion of de afdeling Interne Audit, al naar gelang het geval, kopieën verstrekken van de resultaten van elke audit van het Beleid overeenkomstig Bijlage 1, alsmede alle informatie over de verwerkingsactiviteiten die onder het Beleid vallen, aan elke bevoegde toezichthoudende autoriteit, die bij ontvangst van dergelijke informatie zal worden herinnerd aan haar beroepsgeheim.

1.4 Groepsleden stemmen ermee in dat de bevoegde toezichthoudende autoriteiten een audit of inspectie op het gebied van gegevensbescherming (waar nodig ook ter plaatse) bij hen mogen uitvoeren in overeenstemming met de Europese wetgeving inzake gegevensbescherming van de betreffende Exporterende entiteit.

1.5 Alle Groepsleden gaan ermee akkoord dat zij door de bevoegde toezichthoudende autoriteiten worden gecontroleerd overeenkomstig de toepasselijke controleprocedures van die toezichthoudende autoriteiten.

1.6 Groepsleden stemmen ermee in dat elk geschil met betrekking tot de uitoefening door een bevoegde toezichthoudende autoriteit van haar toezichtsbevoegdheden ten aanzien van dit Beleid zal worden beslecht door de rechtbanken van de lidstaat waar die toezichthoudende autoriteit is gevestigd, overeenkomstig het procesrecht van die lidstaat.

BIJLAGE 4

ACTUALISERINGSPROCEDURE

1. INLEIDING EN ALGEMENE BEGINSELEN

1.1 In deze Actualiseringsprocedure wordt uiteengezet op welke wijze wijzigingen in het Beleid zullen worden meegedeeld aan de bevoegde toezichthoudende autoriteiten, aan betrokkenen en aan Groepsleden die aan het Beleid gebonden zijn.

1.2 Het Beleid zal actueel worden gehouden om recht te doen aan de huidige situatie en context op het gebied van de bescherming van persoonsgegevens.

2. WEZENLIJKE WIJZIGINGEN IN HET BELEID

2.1 De FG van Banco Santander en de juridische afdeling zullen vooraf alle wezenlijke wijzigingen in het Beleid (d.w.z. elke wijziging die mogelijk afbreuk zou doen aan het door het Beleid geboden beschermingsniveau of het Beleid aanzienlijk zou beïnvloeden, zoals wijzigingen in het bindende karakter ervan) meedelen aan het Spaanse bureau voor gegevensbescherming (de "**Leidende toezichthoudende autoriteit voor BCR's**") en, via de Leidende toezichthoudende autoriteit voor BCR's, aan de toezichthoudende autoriteiten. Deze kennisgeving moet een korte toelichting op de redenen voor de actualisering bevatten. De betreffende toezichthoudende autoriteit zal tevens beoordelen of de aangebrachte wijzigingen een nieuwe goedkeuring vereisen.

3. OVERIGE WIJZIGINGEN IN HET BELEID

3.1 De FG van Banco Santander en de juridische afdeling zullen op verzoek, en ten minste eenmaal per jaar, aan de Leidende toezichthoudende autoriteit voor BCR's (en via de Leidende toezichthoudende autoriteit voor BCR's aan de andere betrokken toezichthoudende autoriteiten) mededelen of er wijzigingen in het Beleid zijn aangebracht. Deze jaarlijkse actualisering omvat tevens de hernieuwde bevestiging dat het Aansprakelijke BCR-lid over voldoende activa beschikt, of passende regelingen heeft getroffen om schadevergoeding te kunnen betalen voor schade die voortvloeit uit een inbreuk op het Beleid.

3.2 Voorbeelden van de bovengenoemde wijzigingen zijn onder meer wijzigingen van administratieve aard (waaronder actualiseringen van de lijst van Groepsleden), wijzigingen die het gevolg zijn van een wijziging in de toepasselijke Europese wetgeving inzake gegevensbescherming, of wijzigingen die voortvloeien uit wetgeving, rechterlijke uitspraken of maatregelen en richtsnoeren van toezichthoudende autoriteiten (waaronder richtsnoeren van het Europees Comité voor gegevensbescherming). Banco Santander zal tevens aan de Leidende toezichthoudende autoriteit voor BCR's en aan de overige toezichthoudende autoriteiten een korte toelichting verstrekken over de redenen voor eventuele gemelde wijzigingen in het Beleid.

4. NIEUWE GROEPSLEDEN

4.1 De FG's en Champions (samen met het Privacyteam) zullen ervoor zorgen dat alle nieuwe Groepsleden daadwerkelijk aan het Beleid zijn gebonden en de naleving ervan kunnen waarborgen, voordat een doorgifte van persoonsgegevens aan Groepsleden plaatsvindt.

5. COMMUNICATIE OVER EN REGISTRATIE VAN WIJZIGINGEN IN HET BELEID

5.1 Het Beleid bevat een wijzigingslogboek waarin de datums van herzieningen van het Beleid en de details van aangebrachte wijzigingen worden vermeld. De juridische afdeling houdt een actuele lijst

bij van de wijzigingen die in het Beleid zijn aangebracht en het Corporate DP Office houdt de lijst bij van Groepsleden die hieraan gebonden zijn.

5.2 De juridische afdeling zal, met ondersteuning van het Corporate DP Office, alle wijzigingen in het Beleid communiceren, ongeacht of deze wezenlijk van aard zijn of niet:

(a) aan Groepsleden die aan het Beleid gebonden zijn, zonder onnodige vertraging, en publiceert een bijgewerkte versie van dit Beleid op het interne netwerk van de Santander Groep;

(b) systematisch aan de betrokkenen die baat hebben bij het Beleid, via de website van het bedrijf (Web Corporativa Santander); en

(c) op verzoek en via de betreffende lokale FG's (of soortgelijke functionarissen) aan de bevoegde toezichthoudende autoriteit.