GROUPE SANTANDER

REGLES D'ENTREPRISE CONTRAIGNANTES (REC) – POLITIQUE DU RESPONSABLE DU TRAITEMENT

SOMMAIRE PAGE

INTRODUCTION

Ces Règles d'entreprise contraignantes – Politique du Responsable du traitement et ses Annexes (collectivement, la « **Politique** ») expose l'approche adoptée par Banco Santander, S.A. (« **Banco Santander** ») en ce qui concerne la protection et la gestion des données à caractère personnel par les membres du Groupe Santander –tel que défini ci-après– adhérant à la présente Politique, dans le cadre des transferts internationaux entre Membres du Groupe –tels que définis ci-après– desdites données à caractère personnel.

Banco Santander est la société mère et le siège social de l'un des plus grands groupes financiers d'Espagne, composé à la fois de filiales espagnoles et étrangères (« **Groupe Santander** »), dont l'activité est la fourniture de services financiers à l'échelle mondiale principalement dans les domaines suivants : (i) **Retail & Commercial Banking** : qui englobe l'ensemble des activités de banque de détail et commerciale de Santander ; (ii) **Corporate & Investment Banking** : qui accompagne les clients entreprises et institutionnels avec des services sur mesure et de produits de gros à forte valeur ajoutée, via les divisions Markets, Investment Banking (Global Debt Finance et Corporate Finance) et Global Transactional Banking ; (iii) **Wealth Management & Insurance :** qui regroupe la banque privée, la gestion d'actifs et l'activité d'assurance via Santander Private Banking, Santander Asset Management et Santander Insurance ; (iv) **Digital Consumer Bank** : qui réunit la plateforme numérique Openbank et Santander Consumer Finance afin de créer un modèle unique sur l'ensemble des marchés pour les activités destinées aux consommateurs et l'auto-financement ; et (v) **PagoNxt & Cartes** : qui englobe PagoNxt, et regroupe l'ensemble des activités de paiement de Santander, et Global Cards, l'activité et la plateforme cartes de Santander, proposant des options de paiement numérique et des solutions technologiques globales pour les banques de Santander et de nouveaux clients. En outre, en complément de ce qui précède, le Groupe Santander est également constitué du **Corporate Centre et d'autres fonctions au service de l'ensemble du Groupe** : il s'agit des entités chargées d'apporter soutien et assistance aux Membres du Groupe pour toutes les actions nécessaires au niveau du Groupe qui ne sont pas strictement liées à leur activité principale (par exemple, gestion du personnel, respect des obligations légales, audits, gestion des risques, etc.).

Outre les autres définitions prévues dans la présente Politique, les termes suivants s'appliquent :

« **Législation locale en matière de PD applicable** » désigne toute loi nationale/locale en matière de protection des données (y compris, le cas échéant, la Législation européenne en matière de protection des données) applicable aux Membres du Groupe, pour autant qu'elle respecte l'essence des droits et libertés fondamentaux et ne dépasse pas ce qui est nécessaire et proportionné dans une société démocratique, conformément aux exigences de la Règle 13 de la présente Politique ;

« **autorité de contrôle compétente** » désigne l'autorité de contrôle de l'EEE compétente pour l'Entité exportatrice ;

« **responsable du traitement** » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel ;

« **Europe** » ou « **EEE** » désigne les pays de l'Espace économique européen ;

«**Législation européenne en matière de protection de données**» désigne le RGPD et toute loi sur la protection des données d'un État membre de l'Union européenne, y compris la législation locale, mettant en

œuvre les exigences du RGPD, telle que la réglementation d'application, dans chaque cas avec les modifications introduites de temps à autre ;

« **Entité exportatrice** » désigne un Membre du Groupe établi en Europe, ou autrement soumis à la Législation européenne en matière de protection de données, qui transfère, ou met autrement à la disposition d'une Entité importatrice, des données à caractère personnel en vertu de la présente Politique ;

« **RGPD** » désigne le règlement (UE) 2016/679 (le Règlement général sur la protection des données) ;

« **Membre du Groupe** » désigne les membres du Groupe Santander ayant adhéré à la présente Politique ;

« **Entité importatrice** » désigne un Membre du Groupe établi en dehors de l'Europe qui reçoit des données à caractère personnel d'une Entité exportatrice et traite les données à caractère personnel transférées en dehors de l'EEE ;

« **Membre soumis aux REC responsable** » désigne Banco Santander (c'est-à-dire, Banco Santander S.A., tel que défini ci-dessus) ;

« **données à caractère personnel** » désigne toute information se rapportant à une personne physique identifiée ou identifiable. Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

« **traitement** » désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

« **sous-traitant** » désigne une personne physique ou morale, une autorité publique, un service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

« **profilage** » désigne toute forme de traitement automatisé de données à caractère personnel pour évaluer des aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou les intérêts, la fiabilité ou le comportement, la localisation ou les déplacements de cette personne physique ;

« **catégories particulières de données à caractère personnel** » ou « **données sensibles** » désigne les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, les données génétiques, les données biométriques traitées aux fins d'identifier de manière unique une personne physique, les données concernant la santé ou les données concernant la vie sexuelle d'une personne physique ou son orientation sexuelle ; et

« **autorité de contrôle** » désigne une autorité publique indépendante, instituée dans une juridiction européenne par un État membre, chargée de surveiller l'application de la Législation européenne en matière de protection de données afin de protéger les droits et libertés fondamentaux des personnes physiques à l'égard du traitement et de faciliter la libre circulation des données à caractère personnel au sein de l'EEE.

La présente Politique s'applique à toutes les données à caractère personnel soumises à la Législation européenne en matière de protection de données, qui sont ensuite transférées des Entités exportatrices aux Entités importatrices, ainsi qu'aux transferts ultérieurs des Entités importatrices vers d'autres Entités importatrices ou vers des tiers en dehors de l'EEE (conformément aux exigences prévues à la Règle 6 ci-dessous). Par conséquent, toutes les obligations et exigences assignées aux Membres du Groupe en vertu de la présente Politique seront applicables dans la mesure où elles se rapportent aux données à caractère personnel qui relèvent de ce champ d'application.

La présente Politique s'applique à toutes les données à caractère personnel traitées par les Membres du Groupe, comme indiqué dans les sections « *Quelles données à caractère personnel cette Politique couvre-t-elle ?* » et « *À quelles fins les données à caractère personnel sont-elles transférées au titre de la présente Politique ?* ».

Les Membres du Groupe et leurs salariés doivent se conformer pleinement à la présente Politique et la respecter dans le cadre du traitement de données à caractère personnel au titre de la présente Politique.

La présente Politique vient en complément et ne remplace ni ne se substitue à aucune exigence ou règle spécifique relative à la confidentialité ou au secret, applicable à un domaine d'activité ou à une fonction au sein du Groupe Santander, ou imposée par la législation applicable (pour autant que cette législation soit conforme aux exigences prévues par la Règle 13 ci-après).

La présente Politique, ainsi que la liste des Membres du Groupe actuels et leurs coordonnées figurant à l'Annexe 5, est publiée sur le site web de l'entreprise, accessible au public **ici.**

Application aux transferts effectués par les Membres du Groupe non soumis à la Législation européenne en matière de protection de données

Si un Membre du Groupe non soumis à la Législation européenne en matière de protection de données est également objet de restrictions pour les transferts internationaux de données à caractère personnel en vertu de sa Législation locale en matière de protection des données applicable et que les autorités locales de ces pays reconnaissent la présente Politique (en tout ou partie, selon ce qu'exige la Législation locale en matière de PD applicable) en tant que mécanisme valable permettant de légitimer les transferts internationaux de données à caractère personnel, la présente Politique peut également s'appliquer aux données à caractère personnel transférées depuis ces pays vers les Entités importatrices. Dans un souci de clarification, ceci est sans préjudice de l'application au Membre du Groupe situé en dehors de l'Europe de sa Législation locale en matière de PD applicable.

Dans ces cas, les définitions ci-dessus doivent être interprétées comme considérant le Membre du Groupe qui transfert des données à caractère personnel non soumis à la Législation européenne en matière de protection de données comme l'Entité exportatrice. En conséquence, la Politique doit être interprétée et appliquée *mutatis mutandis* (par exemple, la Législation européenne en matière de protection de données doit être interprétée comme la Législation locale en matière de PD applicable, l'autorité de contrôle compétente comme l'autorité locale compétente dans la juridiction concernée ou l'État membre comme le pays concerné).

Dans ce contexte, le Membre du Groupe qui transfère des données à caractère personnel non soumis à la Législation européenne en matière de protection de données agira en tant que Membre soumis aux REC responsable à l'égard de tels transferts internationaux de données.

PARTIE I : CONTEXTE ET ACTIONS

QU'EST-CE QUE LA LEGISLATION EUROPEENNE EN MATIERE DE PROTECTION DE DONNEES ?

La Législation européenne en matière de protection de données confère aux personnes le droit de contrôler la manière dont leurs données personnelles sont traitées. En vertu de la Législation européenne en matière de protection de données, lorsqu'une organisation traite des données à caractère personnel à ses propres fins, cette organisation est réputée être le responsable du traitement de ces informations et est donc principalement responsable du respect des obligations légales. Par exemple, lorsque nous agissons en tant qu'employeur, nous sommes le responsable du traitement des données à caractère personnel de nos salariés que nous traitons.

En revanche, lorsqu'une organisation traite des informations pour le compte d'une autre entité (par exemple, pour fournir un service), la première est considérée comme un sous-traitant des données.

COMMENT LA LEGISLATION EUROPEENNE EN MATIERE DE PROTECTION DE DONNEES AFFECTE-T-ELLE LES TRANSFERTS DE DONNEES A CARACTERE PERSONNEL ENTRE LES MEMBRES DU GROUPE ?

La Législation européenne en matière de protection de données n'autorise pas les transferts de données à caractère personnel vers des pays, territoires ou organisations internationales situés en dehors de l'Europe qui ne garantissent pas un niveau de protection adéquat des droits des personnes en matière de protection des données. Étant donné que certains des pays dans lesquels les Membres du Groupe exercent leurs activités ne sont pas considérés par la Commission européenne comme offrant un niveau de protection adéquat, des garanties appropriées doivent être mises en place afin de répondre aux exigences de la Législation européenne en matière de protection de données.

QUE FONT LES MEMBRES DU GROUPE A CE SUJET ?

Les Membres du Groupe doivent prendre les mesures appropriées pour garantir que le traitement des données à caractère personnel, lors de leur transfert à l'international, est sécurisé et licite. L'objet de la présente Politique est donc d'établir un cadre permettant de satisfaire aux normes prévues par la Législation européenne en matière de protection de données et, par conséquent, d'assurer un niveau de protection adéquat pour l'ensemble des données à caractère personnel transférées des Entités exportatrices vers les Entités importatrices.

La présente Politique est juridiquement contraignante et s'applique à tous les Membres du Groupe et à leurs employés lorsque ces Membres du Groupe traitent des données à caractère personnel, tant manuellement que par des moyens automatisés. Elle exige que les Membres du Groupe se conforment aux Règles énoncées dans la Partie II de la présente Politique (le cas échéant), ainsi qu'aux politiques et procédures énoncées dans les Annexes de la Partie III de la présente Politique. Si une Entité importatrice est soumise à une Législation locale en matière de PD applicable qui est reconnue comme offrant un niveau de protection adéquat en vertu de la Législation locale en matière de PD applicable de l'Entité exportatrice et qui assure un niveau de protection équivalent à celui décrit dans la présente Politique, les processus et procédures locaux qui se conforment pour l'essentiel aux exigences de la présente Politique seront considérés comme valides, même s'ils introduisent des variations ou des différences procédurales (par exemple, des équipes locales chargées de certaines procédures), pour autant que ces variations soient conformes à la présente Politique. Les transferts internationaux couverts par la présente Politique comprennent les transferts de données à caractère personnel provenant de Membres du Groupe qui relèvent du champ d'application territorial du RGPD, conformément à l'article 3 du RGPD, vers des Membres du Groupe situés en dehors de l'EEE, ainsi que des transferts ultérieurs à destination d'autres Membres du Groupe ou de tiers externes (conformément aux exigences énoncées dans la Règle 6 ci-dessous) en dehors de l'EEE.

QU'EN EST-IL DES MEMBRES DU GROUPE NON SOUMIS A LA LEGISLATION EUROPEENNE EN MATIERE DE PROTECTION DE DONNEES QUI EXPORTENT DES DONNEES ?

Comme expliqué dans l'introduction, et aux fins de concevoir un cadre mondial de protection des données pour le Groupe Santander, si un Membre du Groupe non soumis à la Législation européenne en matière de protection de données a également des restrictions pour les transferts internationaux de données à caractère personnel en vertu de sa Législation locale en matière de protection des données applicable et que les autorités locales de ces pays reconnaissent la présente Politique (en tout ou partie, selon ce qu'exige la Législation locale en matière de PD applicable) en tant que mécanisme valable permettant de légitimer les transferts internationaux de données à caractère personnel, la présente Politique peut également s'appliquer aux données à caractère personnel transférées depuis ces pays vers les Entités importatrices. Dans un souci de clarification, ceci est sans préjudice de l'application au Membre du Groupe situé en dehors de l'Europe de sa Législation locale en matière de PD applicable.

QUELLES DONNEES PERSONNELLES CETTE POLITIQUE COUVRE-T-ELLE ?

Les données à caractère personnel traitées dans le cadre de la présente Politique comprennent ce qui suit :

- En ce qui concerne les données à caractère personnel des **actuels et anciens salariés et autres membres du personnel (tels que les stagiaires, les détachés ou les travailleurs indépendants)** :

  (a) données personnelles et coordonnées de contact (par exemple, prénom, deuxième prénom, nom de famille, titre, pseudonyme, signature, sexe, date de naissance, nationalité, numéros/documents d'identification nationaux, adresse e-mail, adresse du domicile, numéros de téléphone, photographie, permis de travail, etc.) ; **(b) données d'emploi y compris l'historique professionnel, les conditions de travail et les coordonnées** (par exemple, adresse e-mail et numéro de téléphone professionnels de l'entreprise, numéro d'identification de l'employé, attribution du nom d'utilisateur/de la clé d'adresse (utilisée pour l'accès aux terminaux de poste de travail), historique professionnel, poste actuel, rôle, tâches, société, centre d'affaires, unité opérationnelle, numéro d'identification du département, numéro d'identification de la succursale, pays d'activité, identifiant(s) et nom(s) du(des) superviseur(s), identifiant(s) et nom(s) du(des) subordonné(s), statut et type d'emploi, indication de si l'employé est externe, date d'embauche, date de début de poste, (le cas échéant) date de fin de contrat, données contractuelles, régimes de retraite, flexibilité du travail, demandes de mobilité, dotation, données de conformité aux politiques internes ou autres dispositions légalement applicables, évaluations de performance et qualifications (y compris les retours des managers, des parties prenantes et d'autres personnes qui travaillent avec l'employé), promotions et dossiers disciplinaires, etc.) ; **(c) détails relatifs au talent, au recrutement et aux candidatures, à l'éducation et à la formation** (par exemple, détails figurant dans les lettres de candidature et le CV, détails relatifs au plan de développement et à l'évaluation, détails de formation, site web personnel ou profil LinkedIn fournis directement par les employés, antécédents d'emploi et références antérieures, parcours éducatif et de formation, qualifications professionnelles, compétences linguistiques et autres compétences pertinentes, etc.) ; **(d) informations financières, y compris les détails de paie et de rémunération** (par exemple, coordonnées bancaires, salaire, régimes d'avantages, primes, devise, rémunération variable, détails sur les options sur actions, attributions d'actions et autres attributions, fréquence de paiement, date d'effet de la rémunération actuelle, révisions salariales, identifiant fiscal et code fiscal, etc.) ; **(e) détails relatifs à la sécurité et à l'informatique** (par exemple, identifiant d'utilisateur, clé d'accès aux outils, connexions, informations d'identification et profils de sécurité, e-mails transmis depuis et reçus sur les comptes de messagerie de l'entreprise (dans la mesure légalement permise), informations capturées via l'utilisation des systèmes informatiques, y compris les informations d'accès et d'authentification, historique de navigation Internet, numéros de téléphone composés, documents et fichiers stockés sur les systèmes ou réseaux de l'entreprise (y compris les bureaux des ordinateurs), journaux, adresse IP, tentatives de connexion réussies et échouées, informations collectées via des *cookies* ou d'autres

technologies de suivi similaires, etc.) ; **(f) données relatives aux horaires de travail** (par exemple, congés, jours et temps de repos, autres congés et justificatifs des motifs (le cas échéant), dates de réintégration après les congés, autres données d'absence, enregistrement des heures travaillées (lorsque légalement requis/autorisé), heures supplémentaires, horaire d'équipe, etc.) ; et **(g) toute autre information fournie volontairement par les personnes concernées** (par exemple, via des enquêtes d'engagement ou d'autres enquêtes, etc.).

En outre, des **catégories particulières de données à caractère personnel** (**notamment, mais pas uniquement, les données concernant la santé et l'appartenance à un syndicat**) peuvent être traitées par les Membres du Groupe lorsque cela est nécessaire et requis ou autorisé par la loi applicable aux fins décrites dans la section suivante.

- Concernant **les membres de la famille des employés** et leurs données à caractère personnel :

  (a) données personnelles et coordonnées (par exemple, prénom, nom de famille, sexe, numéros d'identification nationaux /documents d'identité, coordonnées telles que le numéro de contact d'urgence, etc.) ; et **(b) autres informations concernant les employés, ou concernant leur famille, lorsque cela est légalement requis/autorisé** (par exemple, composition et situation de la famille, lien avec l'employé, nom et autres informations pertinentes concernant les enfants et autres personnes à charge, état civil, données relatives au respect des politiques internes ou d'autres règles légalement applicables, etc.).

- Concernant les données personnelles des **candidats actuels et anciens** :

  (a) données personnelles et coordonnées (par exemple, prénom, nom de famille, pays, état et ville de résidence, adresse e-mail, adresse du domicile, numéros de téléphone, nationalité, etc.) ; **(b) données relatives au recrutement, aux études et à la formation** (par exemple, renseignements figurant dans les lettres de candidature et le curriculum vitæ (CV), site web personnel ou profil LinkedIn fournis directement par les candidats, antécédents professionnels et références, parcours d'études, qualifications professionnelles, compétences linguistiques et autres compétences pertinentes, détails relatifs aux évaluations de performance, plan de développement et disposition à la mobilité géographique, données personnelles issues de la participation des candidats au processus de recrutement, telles que, par exemple, celles obtenues lors d'entretiens personnels et les e-mails échangés concernant les candidatures ou les conversations, etc.) ; et **(c) informations audio et visuelles** (par exemple, la voix et l'image telles que captées dans des photographies, des enregistrements vidéo ou audio dans le cadre d'entretiens menés par téléphone ou par visioconférence, etc.).

- S'agissant des **prospects, acheteurs et clients**, les données à caractère personnel (y compris celles de leurs employés, représentants et/ou agents, le cas échéant, des utilisateurs autorisés et des utilisateurs du site web) :

  (a) données personnelles et coordonnées (par exemple, prénom, deuxième prénom, nom de famille, numéro de téléphone, adresse e-mail, adresse postale, pays de résidence, région, citoyenneté ou nationalité, numéros/documents d'identification nationaux, sexe, langue, date de naissance, pays de naissance, état civil, données relatives à la situation familiale ou sociale (par exemple, nombre de personnes à charge), indication si la personne est mineure ou nécessite un représentant légal, données démographiques et socioéconomiques, etc.) ; **(b) données professionnelles** (par exemple, profession, poste, antécédents professionnels et académiques, informations sur l'entreprise, coordonnées professionnelles, métier, catégorie professionnelle, intitulé de poste, etc.) ; **(c) données (pré)contractuelles** (par exemple, code de catégorie, capacité juridique, données relatives à la procuration, numéro d'enregistrement et indicateur interne du client, niveau d'engagement, relation

d'affaires avec Santander, produits ou services souscrits ou demandés, score de risque, informations issues des agences de crédit, bons de commande, données statistiques, factures, informations sur les biens et les actifs, subventions, informations sur les comptes et les opérations, dans la mesure permise par la loi applicable, contrats et autres accords pouvant contenir des données à caractère personnel des personnes concernées et leur performance, etc.) ; **(d) informations financières, fiscales et de paiement** (par exemple, coordonnées bancaires, informations sur le bénéficiaire, soldes actuels et historiques des produits et services et historique des paiements, détails de la carte de crédit, versement direct de la paie, détails/type de revenus, fonds disponibles, transactions monétaires, montant du paiement, détails du virement, informations sur la solvabilité, numéro d'identification fiscale, pays de résidence fiscale, solde fiscal annuel, etc.) ; **(e) données de conformité** (par exemple, identifiant PEP lié, relation MiFID ou similaire (par exemple, associés, liens familiaux, etc.), type de relation (par exemple, conjoint, proche, actionnaire, représentants légaux, etc.), date de début de la relation et (le cas échéant) date de fin, informations relatives aux obligations de lutte contre le blanchiment de capitaux et la fraude (profils, informations et scores issus des bases de données de solvabilité et de risques, etc.) ; **(f) informations audio et visuelles** (par exemple, voix et image telles que capturées dans des photographies, des vidéos ou des enregistrements audio dans le cadre de réunions tenues par téléphone ou par visioconférence, ou à des fins de sécurité, etc.) ; **(g) informations informatiques** (par exemple, adresse IP, identifiant d'utilisateur, mots de passe, *logs* (y compris les détails de profil) des sites web ou portails du Groupe Santander, clé d'accès aux outils, informations d'identification et profils de sécurité, données d'authentification informatique, historique de navigation, identifiant de l'appareil, identifiant publicitaire, réseaux sociaux, etc.) ; et **(h) autres détails concernant la relation professionnelle avec le Groupe Santander** (par exemple, données relatives aux réclamations, communications partagées, préférences de communication, demandes, etc.).

En outre, **des catégories particulières de données à caractère personnel (y compris les données à caractère personnel relatives aux condamnations pénales et aux infractions –dans le cadre des risques et sanctions internationaux–**) peuvent être traitées par les Membres du Groupe lorsque cela est nécessaire et exigé ou autorisé par la loi applicable aux fins décrites dans la section suivante.

- Concernant les données à caractère personnel des **fournisseurs ou prestataires potentiels et actuels** (y compris celles de leurs employés, représentants et/ou agents, le cas échéant) :

  (a) données personnelles, professionnelles et de contact (par exemple, prénom, nom de famille, numéro de téléphone, adresse e-mail, adresse postale, numéros/documents d'identification nationaux, poste/intitulé du poste, informations sur l'entreprise, coordonnées professionnelles, etc.) ; **(b) données contractuelles** (par exemple, données relatives à une procuration, bons de commande, factures, contrats et autres accords susceptibles de contenir des données personnelles concernant ces personnes concernées, etc.) ; **(c) informations financières et de paiement** (par exemple, coordonnées bancaires, données de carte de crédit, informations sur la solvabilité, etc.) ; **(d) informations audio et visuelles** (par exemple, voix et image telles que capturées sur des photographies, des vidéos ou des enregistrements audio dans le cadre de réunions tenues par téléphone ou via visioconférence, ou à des fins de sécurité (y compris les informations capturées par des systèmes d'accès et des caméras de sécurité), etc.) ; **(e) informations informatiques** (par exemple, adresse IP, identifiant d'utilisateur, mots de passe, *logs* (y compris les détails de profil) des sites web ou portails du Groupe Santander, etc.) ; et **(f) autres détails concernant la relation professionnelle avec le Groupe Santander** (par exemple, données relatives aux réclamations, communications partagées, etc.).

- Concernant les données à caractère personnel des **actionnaires** :

  (a) données personnelles, professionnelles et de contact (par exemple, nom, prénom, sexe, date de naissance, numéro de téléphone, adresse e-mail, adresse postale, numéros/documents d'identification nationaux, poste/intitulé du poste, informations sur l'entreprise, coordonnées professionnelles, numéro

d'actionnaire, nationalité/citoyenneté, pays de naissance et de résidence, etc.) ; **(b) informations financières et de paiement** (par exemple, coordonnées bancaires, données de carte bancaire, informations de paiement, nombre d'actions, documents de propriété et de dividendes, transactions monétaires, mouvements, positions et détenteurs d'actions dans d'autres sociétés, informations sur les produits financiers souscrits, etc.) ; et **(c) informations informatiques** (par exemple, adresse IP, identifiant utilisateur, mots de passe, *logs* (y compris les détails du profil) des sites web ou des portails du Groupe Santander, etc.).

- En ce qui concerne les données à caractère personnel des **utilisateurs Internet, utilisateurs finaux et utilisateurs institutionnels (y compris ceux des plateformes/sites web/applications liés aux universités, à l'emploi et à l'entrepreneuriat) :**

  (a) **données personnelles et coordonnées** (par exemple, nom, prénom, date de naissance, sexe, adresse e-mail, adresse postale, numéros de téléphone, pays de résidence, nationalité, numéros d'identification nationaux, etc.) ; **(b) données professionnelles et éducatives** (par exemple, poste/intitulé du poste, informations sur l'entreprise, coordonnées professionnelles, parcours professionnel, CV, données académiques, formation ou diplômes, données démographiques et socioéconomiques, liens avec des projets entrepreneuriaux ou des entreprises, etc.) ; **(c) informations informatiques** (par exemple, adresse IP, identifiant utilisateur, mots de passe, journaux d'utilisation (y compris les détails du profil) des sites web ou portails, enregistrements d'appels, etc.) ; **(d) données de navigation et d'utilisation** (par exemple, informations collectées automatiquement auprès des personnes concernées (via des *cookies* ou d'autres technologies similaires) concernant leur utilisation de sites web/appareil (y compris les profils), navigation sur le web, données d'utilisation, etc.) ; et **(e) autres détails concernant leur relation avec le Groupe Santander** (par exemple, demandes, centres d'intérêt, communications échangées, etc.)

À QUELLES FINS LES DONNEES A CARACTERE PERSONNEL SONT-ELLES TRANSFEREES DANS LE CADRE DE LA PRESENTE POLITIQUE ?

Les données à caractère personnel sont transférées entre les Membres du Groupe à l'échelle mondiale (principalement en Argentine, aux Bahamas, au Brésil, en Colombie, dans des pays d'Europe, au Mexique, au Pérou, en Suisse, au Royaume-Uni, aux États-Unis d'Amérique, en Uruguay, etc.) en vertu de la présente Politique aux fins suivantes et uniquement dans la mesure permise par les lois applicables :

- Les transferts de données à caractère personnel des **actuels et anciens employés et autres membres du personnel (tels que stagiaires, personnes en détachement ou travailleurs indépendants)** sont effectués aux fins suivantes : **(a) administration et gestion du personnel** (par exemple, gestion des formations, planification et suivi, gestion des performances, gestion de la paie et des avantages, promotions, planification de la relève et développement de carrière, gestion de la mobilité interne, transferts et détachements, élaboration et gestion des annuaires d'employés existants, organisation des déplacements professionnels, gestion des frais professionnels et des remboursements, facilitation des communications, négociations, transactions et conférences professionnelles, vérification du respect par l'employé de ses obligations et devoirs professionnels, congés et absences, évaluations, gestion et déclaration des mesures disciplinaires et des cessations d'emploi, réexamen des décisions en matière d'emploi, constatation et prise de décisions relatives à l'aptitude des employés au travail et aux aménagements du lieu de travail, contrôle du respect des politiques et procédures internes et autres activités de surveillance requises par les lois applicables (par exemple, systèmes de signalement internes), y compris le respect du Code de conduite sur les marchés de valeurs mobilières ou de politiques similaires et obligations connexes, y compris l'approbation et le suivi des opérations sur compte personnel, réalisation d'analyses et de planification de la main-d'œuvre, réalisation de vérifications d'antécédents comme l'exigent ou l'autorisent les lois applicables, etc.) ; **(b) réalisation de segmentations, statistiques et analyses agrégées** concernant les données d'activité des employés afin

d'améliorer la compréhension de la population des employés et d'éclairer les décisions la concernant, notamment en matière de recrutement de talents, de planification de carrière et de planification de la relève ; **(c) soutien à la gestion des services fournis par le Groupe Santander et de ses activités** (par exemple, gestion et sécurisation des systèmes et infrastructures informatiques et de communication, gestion et affectation des actifs de l'entreprise et des ressources humaines, des équipements de bureau et des autres biens, planification opérationnelle et stratégique, gestion de projets, continuité d'activité, constitution de pistes d'audit et autres outils de *reporting*, tenue de registres relatifs aux activités de l'entreprise, budgétisation, gestion financière et *reporting*, communications, gestion des fusions, acquisitions, et des réorganisations ou cessions, etc.) ; et **(d) respect des obligations légales applicables et autres exigences** (par exemple, obligations en matière de protection des données, fiscales et de sécurité sociale, prévention des risques et droit du travail, prévention de la fraude, dispositifs d'alerte professionnelle, obligations de tenue de registres et de déclaration, exercice de droits et recours juridiques, défense en justice, assurer la conformité lors des inspections gouvernementales et autres demandes émanant des autorités publiques, répondre aux procédures judiciaires telles que les assignations, obligations en matière de travail et de sécurité sociale, réalisation d'audits, et gestion de toute plainte ou réclamation interne, etc.).

En ce qui concerne les **catégories particulières de données à caractère personnel des salariés (y compris les données à caractère personnel relatives aux condamnations pénales et aux infractions, lorsque la loi l'autorise)**, ces données peuvent être traitées par les Membres du Groupe si nécessaire afin de remplir dûment leurs finalités (par exemple, le respect des obligations légales, la gestion des ressources humaines, la gestion du dispositif d'alerte, la gestion de la paie et des avantages sociaux, l'administration de la mobilité interne, des transferts et des détachements, la réalisation de segmentations agrégées, de statistiques et d'analyses, etc.) et uniquement dans la mesure nécessaire aux fins de l'exécution des obligations et de l'exercice de droits spécifiques des Membres du Groupe ou de la personne concernée dans le domaine du droit du travail, de la sécurité sociale et de la protection sociale (article 9, paragraphe 2, lettre b), du RGPD) ainsi qu'aux fins de la médecine préventive ou de la médecine du travail, de l'évaluation de la capacité de travail du salarié, du diagnostic médical, de l'administration de soins ou traitements de santé ou sociaux, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale (article 9, paragraphe 2, lettre h), du RGPD).

- Des transferts de données personnelles des **membres de la famille des salariés** sont effectués aux fins de la gestion des affectations de salariés à l'étranger et de la réalisation de segmentations, de statistiques et d'analyses agrégées, ainsi que pour la surveillance du respect du Code de conduite sur les marchés de valeurs mobilières ou de politiques similaires et des obligations connexes, y compris l'approbation et le suivi des transactions sur compte personnel, ainsi que pour la gestion des prestations sociales relatives aux droits des salariés (par exemple, dans le cadre d'assurances).

- Les transferts de données personnelles des **candidats actuels et anciens** sont effectués aux fins de la gestion des activités de recrutement nationales/internationales (par exemple, pour évaluer les candidatures et prendre des décisions d'embauche, communiquer avec les candidats concernant le processus de recrutement et/ou leur(s) candidature(s), etc.).

- Les transferts de données personnelles de **prospects, acheteurs et clients** (y compris celles de leurs salariés, représentants et/ou mandataires, utilisateurs autorisés et utilisateurs du site web) sont effectués aux fins de : **(a) gérer la relation contractuelle avec eux et fournir nos services** (par exemple, émission de cartes de paiement, y compris aux utilisateurs autorisés d'une carte d'entreprise, offre et gestion de nos services de paiement et de banque en ligne, tenue de registres afin d'assurer l'alignement des informations entre les juridictions, mise en place d'accords et/ou prise de mesures pour conclure de tels accords (procédures de connaissance du client, KYC), à des fins professionnelles et de communication, transferts de compte, établissement, renouvellement, maintien ou résiliation des relations d'affaires, fourniture d'accès aux activités en ligne et à nos locaux, tenue des registres

commerciaux, réalisation d'audits, de comptabilité et d'analyses financières et économiques, exécution de fonctions de paiement et de comptabilité associées, évaluation du risque et du crédit/de la solvabilité, etc.) ; **(b) gérer et garantir la sécurité** (par exemple, protection de l'infrastructure informatique, des équipements de bureau et autres biens, etc.) ; **(c) gérer les opérations commerciales** (par exemple, tenue de registres des représentants des entreprises ou d'autres coordonnées de points de contact, assurer l'alignement des opérations entre les juridictions, tenue de registres des réunions et d'autres relations d'affaires, exploitation et gestion des systèmes informatiques et de communication, gestion du développement de produits et de services, amélioration des produits et services, gestion des actifs de l'entreprise, planification stratégique, gestion de projet, continuité d'activité, constitution de pistes d'audit et autres outils de *reporting*, etc.) ; **(d) se conformer à la législation applicable** (par exemple, obligations en matière de protection des données et fiscales, MiFID et évaluation de l'adéquation et du caractère approprié des produits d'investissement, prévention de la fraude, lutte contre le blanchiment d'argent, obligations de tenue de registres et de déclaration, exercice de droits et de recours juridiques, défense en cas de différends ou de contentieux, respect des inspections gouvernementales et autres demandes émanant du gouvernement ou d'autres autorités publiques, réponse aux procédures judiciaires telles que les assignations à comparaître, etc.) ; et **(e) planifier et exécuter des stratégies ou des campagnes marketing** (par exemple, études de marché, planification de campagnes et élaboration de stratégies marketing, suivi et *reporting* sur la réussite des campagnes, ciblage de produits/services (y compris le profilage), lorsqu'il y a consentement ou lorsque la loi l'autorise, etc.).

S'agissant des **catégories particulières de données à caractère personnel (y compris les données à caractère personnel relatives aux condamnations pénales et aux infractions, lorsque cela est autorisé**) des clients (y compris celles de leurs employés, représentants et/ou agents), ces données peuvent être traitées par les Membres du Groupe si cela est nécessaire afin de remplir correctement leurs finalités (par exemple, le respect des obligations légales, l'identification d'informations accessibles au public concernant les pratiques de clients d'autres entités susceptibles d'affecter leur relation avec la société ; l'alignement des informations entre juridictions, le respect des inspections gouvernementales ou judiciaires et d'autres demandes émanant d'autres autorités publiques, etc.) et uniquement dans la mesure nécessaire aux fins d'exécuter les obligations des Membres du Groupe ou de la personne concernée dans les domaines de la lutte contre le blanchiment de capitaux, de la prévention de la fraude, de la prévention de la criminalité et des domaines connexes (lorsque cela est nécessaire et requis ou autorisé par la législation applicable).

- Les transferts de données à caractère personnel des **fournisseurs ou prestataires potentiels et actuels** (y compris celles de leurs employés, représentants et/ou agents) sont effectués aux fins suivantes : **(a) gérer la relation (pré)contractuelle avec eux ou leur entreprise** (lorsqu'il s'agit de personnes morales) **généralement** (par exemple, effectuer des contrôles des niveaux de normes de qualité, analyse du niveau de risque des fournisseurs, comptabilité, analyse financière et économique, prise de mesures pour conclure des accords pertinents, exécution des accords en vigueur, exécution des paiements et des fonctions comptables associées, à des fins commerciales et de communication, l'établissement, le renouvellement, le maintien ou la cessation des relations d'affaires, tenue des registres commerciaux, etc.) ; **(b) gérer et garantir la sécurité** (par exemple, protection de l'infrastructure informatique, du matériel de bureau et des autres biens, etc.) ; **(c) gérer les opérations commerciales** (par exemple, exploitation et gestion des systèmes informatiques et de communication, gestion du développement des produits et des services, planification stratégique, gestion de projets, continuité d'activité, constitution de pistes d'audit et d'autres outils de *reporting*, tenue des dossiers relatifs aux activités commerciales, budgétisation, gestion financière et *reporting*, communications, etc.) ; et **(d) se conformer à la législation applicable** (par exemple, la législation commerciale, fiscale, de prévention de la fraude, obligations d'externalisation lorsqu'elles sont effectuées par des entités financières, réalisation d'audits, conformité aux inspections et autres demandes des autorités gouvernementales ou autres autorités publiques, exercice de droits et de recours juridiques, défense en justice et gestion de toute réclamation ou plainte interne, etc.).

- Les transferts de données à caractère personnel des **actionnaires** sont effectués aux fins suivantes : **(a) gestion de la relation avec l'actionnaire** (par exemple, à des fins commerciales et de communication, établissement, renouvellement, maintien ou résiliation des relations d'affaires, organisation des assemblées annuelles et gestion des droits de l'actionnaire, paiement de dividendes, tenue des registres commerciaux, fourniture d'un accès aux activités en ligne et aux locaux, etc.) ; et **(b) respect de la législation applicable** (par exemple, lois commerciales et sur les sociétés, lois fiscales et sur les valeurs mobilières, réalisation d'audits, conformité aux inspections gouvernementales et autres demandes émanant d'autorités gouvernementales ou autres autorités publiques, respect des obligations en matière de lutte contre le blanchiment de capitaux, certifications, exercice des droits et recours juridiques, défense en justice et gestion de toute plainte ou réclamation interne, etc.

- Les transferts de données à caractère personnel des **utilisateurs du site web, des utilisateurs finaux et des utilisateurs institutionnels (y compris ceux des plateformes/sites web/applications liés aux universités, à l'emploi et à l'entrepreneuriat)** sont effectués aux fins de **(a) gérer de manière générale la fourniture des services** (par exemple, développer et fournir des fonctionnalités et des contenus en ligne, gérer des sites web, traiter les demandes de renseignements et requêtes, fournir une assistance, etc.) ; **(b) gérer et garantir la sécurité** (par exemple, protéger l'infrastructure informatique, assurer la sécurité et l'intégrité des systèmes, des serveurs et des sites web, etc.) ; **(c) gérer les opérations commerciales** (par exemple, assurer l'alignement des opérations entre les juridictions, tenir des registres des réunions et autres relations d'affaires, améliorer à l'échelle mondiale les processus de ressources humaines et d'acquisition de talents, etc.) ; **(d) planifier et exécuter des stratégies ou des campagnes marketing** (par exemple, études de marché, planification des campagnes et élaboration de stratégies marketing, suivi et établissement de rapports sur le succès des campagnes, ciblage de produits/services (y compris le profilage), lorsque cela est consenti ou légalement autorisé, etc.) ; **(e) gérer les activités de recrutement nationales/internationales** (par exemple, évaluer les candidatures et prendre des décisions d'embauche, communiquer avec les candidats en lien avec le processus de recrutement et/ou leur(s) candidature(s), etc.) ; **(f) réaliser des segmentations, des statistiques et des analyses agrégées** (par exemple, pour comprendre comment les services sont utilisés, améliorer et développer les fonctionnalités des sites web et des services, renforcer les performances et l'assistance disponible, etc.) ; et **(g) se conformer à la législation applicable** (par exemple, lois commerciales, réalisation d'audits, respect des inspections gouvernementales et des autres demandes émanant du gouvernement ou d'autres autorités publiques, réponse aux procédures judiciaires telles que des citations à comparaître, exercice de droits et de recours juridiques, assurer la défense dans le cadre de litiges et gérer toute plainte ou réclamation interne, etc.).

Les données à caractère personnel visées par la présente Politique sont également transférées entre les Membres du Groupe selon les besoins aux fins de la **prestation d'un large éventail de services internes entre eux** (par exemple, technologies et systèmes informatiques, services de *back-office*, sélection et gestion des ressources humaines, audit interne et conformité, gestion du canal d'alerte, service central de courrier pour les candidatures et les employés, services de technologie et de traitement des paiements, services d'autorisation et de capture des cartes de crédit, services de facturation et de tarification, destruction de documents, transport de documents, gestion des risques, approvisionnement en produits et/ou services, facturation électronique, gestion du marketing et de la communication, ainsi que des services de gestion juridique et de coordination dans certains domaines tels que la protection des données, etc.)

INFORMATIONS COMPLEMENTAIRES

Le Groupe Santander a nommé des DPD locaux et/ou des Champions (tels que ces termes seront définis ci-dessous) qui dirigent les équipes locales, veillent à la conformité locale au sein des différentes entités dans le monde entier et font partie de l'Équipe de protection de la vie privée du Groupe Santander (également définie ci-dessous). Si vous avez des questions concernant les dispositions de la présente Politique, vos droits au titre de cette Politique ou toute autre question relative à la protection des données, vous pouvez contacter le

DPD/Champion concerné à l'adresse indiquée ci-dessous. Le DPD/Champion traitera la question, la transmettra à la personne ou au service approprié au sein du Groupe Santander ou, le cas échéant, fera remonter la question à la personne/instance correspondante.

À l'attention : Équipe de protection de la vie privée

E-mail : La liste des adresses e-mail pertinentes est disponible ici.

Si vous avez des soucis concernant la manière dont un Membre du Groupe a pu traiter vos données personnelles, il existe une procédure spécifique de traitement des réclamations décrite dans la Partie III (cf. **Annexe 2**).

PARTIE II : OBLIGATIONS DES MEMBRES DU GROUPE

La Partie II de la présente Politique est divisée en trois sections :

- La Section A traite des principes fondamentaux de protection des données, conformes à ceux prévus par la Législation européenne en matière de protection de données, que doit respecter un Membre du Groupe.

- La Section B traite des engagements pratiques pris par les Membres du Groupe envers les autorités de contrôle compétentes dans le cadre de la présente Politique.

- La Section C décrit les droits des tiers bénéficiaires que les Membres du Groupe ont accordés aux personnes concernées au titre de la Partie II de la présente Politique.

SECTION A : PRINCIPES DE BASE

RÈGLE 1 – LICÉITÉ ET LOYAUTÉ

Règle 1A – Les Membres du Groupe se conformeront à cette Politique et à toute Législation locale en matière de PD applicable de manière harmonisée.

En tant qu'organisations, les Membres du Groupe, sous réserve de ce qui suit, se conformeront à toute législation applicable relative aux données à caractère personnel (par exemple, en Europe, la Législation européenne en matière de protection de données) et veilleront à ce que, lorsque des données à caractère personnel sont traitées, ce traitement soit effectué conformément à la présente Politique et à la Législation locale en matière de PD applicable.

Lorsque la présente Politique s'applique et :

- il n'existe aucune Législation locale en matière de PD applicable, ou si la loi ne répond pas aux normes énoncées par les Règles de la présente Politique, la position des Membres du Groupe sera de traiter les données à caractère personnel conformément à la présente Politique, dans le respect des Règles qu'elle énonce ;

- la Législation locale en matière de PD applicable exige un niveau de protection plus élevé que celui prévu par la présente Politique, ce niveau de protection plus élevé prévaudra sur la présente Politique, à condition que les droits et obligations prévus par la présente Politique continuent d'être respectés ; ou

- la Législation locale en matière de PD applicable empêche les Membres du Groupe de s'acquitter de leurs obligations au titre de la présente Politique, ou a une incidence substantielle sur leur capacité à respecter ces obligations, les Membres du Groupe suivront la procédure énoncée dans la Règle 13.

Règle 1B – Les Membres du Groupe veilleront à ce que leur traitement des données à caractère personnel soit loyal et licite et qu'une base juridique existe pour le traitement des données à caractère personnel, le cas échéant.

Les Membres du Groupe veilleront à ce que le traitement de données à caractère personnel qu'ils effectuent soit loyal et licite, et qu'il existe, lorsque cela est requis, une base juridique pour ce traitement. Conformément à la Législation européenne en matière de protection de données, les Membres du Groupe ne traiteront des données à caractère personnel que lorsque :

- la personne concernée a donné son consentement au traitement de ses données à caractère personnel et que ce consentement satisfait aux exigences prévues par la Législation européenne en matière de protection de données (c'est-à-dire, qu'il doit être libre, spécifique, éclairé et univoque) ; ou

- il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, ou pour prendre des mesures à la demande de la personne concernée avant la conclusion d'un contrat ; ou

- il est nécessaire pour se conformer à une obligation légale à laquelle le Membre du Groupe est soumis (pour autant que cette loi respecte les exigences de la Règle 13 ci-après, le cas échéant) ; ou

- il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou

- il est nécessaire à l'exécution d'une mission d'intérêt public ou dans l'exercice de l'autorité publique conférée à un Membre du Groupe (dans la mesure où une telle mission est prévue par une loi conforme aux exigences de la Règle 13 ci-après, le cas échéant) ; ou

- il est nécessaire aux fins des intérêts légitimes poursuivis par un Membre du Groupe ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée.

Lorsque le traitement de données à caractère personnel se rapporte à des condamnations pénales et à des infractions ou à des mesures de sûreté connexes, les Membres du Groupe n'effectueront ce traitement que sous le contrôle de l'autorité publique ou lorsque le traitement est autorisé par la loi prévoyant des garanties appropriées pour les droits et libertés des personnes concernées, conformément aux bases juridiques précitées.

Règle 1C – Sans préjudice de la Règle 1B ci-dessus, le traitement des catégories particulières de données à caractère personnel est interdit, sauf si une dérogation s'applique, par exemple parmi celles prévues par la Législation européenne en matière de protection de données.

Le traitement des catégories particulières de données à caractère personnel n'est autorisé que pour certains motifs :

- Le Membre du Groupe a obtenu le consentement explicite au traitement de toute catégorie particulière de données à caractère personnel de la personne concernée pour une ou plusieurs finalités déterminées sauf si une loi prévoit que l'interdiction de traiter des catégories particulières de données à caractère personnel ne peut être levée par la personne concernée ; ou

- le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits spécifiques du Membre du Groupe ou de la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où il est autorisé par la loi ou par une convention collective conclue en vertu de la loi, prévoyant des garanties appropriées pour les droits fondamentaux et les intérêts des personnes concernées ; ou

- le traitement est nécessaire afin de protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique lorsque la personne concernée est physiquement ou juridiquement incapable de donner son consentement ; ou

- le traitement est effectué, dans le cadre de ses activités légitimes et avec des garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif poursuivant une finalité politique, philosophique, religieuse ou syndicale et à condition que le traitement porte exclusivement

sur les membres ou les anciens membres de l'organisme ou sur des personnes entretenant des contacts réguliers avec celui-ci en relation avec ses finalités et que les données à caractère personnel ne soient pas communiquées à l'extérieur de cet organisme sans le consentement des personnes concernées ; ou

- le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ; ou

- le traitement est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice, ou chaque fois que les juridictions agissent dans l'exercice de leurs fonctions juridictionnelles ; ou

- le traitement est nécessaire pour des motifs d'intérêt public important sur la base d'une loi, à condition qu'il soit proportionné à l'objectif poursuivi, qu'il respecte l'essence du droit à la protection des données et qu'il prévoie des mesures appropriées et spécifiques visant à sauvegarder les droits fondamentaux et les intérêts de la personne concernée ; ou

- le traitement est nécessaire à des fins de médecine préventive ou de médecine du travail, à l'évaluation de la capacité de travail du salarié, au diagnostic médical, à la prise en charge sanitaire ou sociale, ou à la gestion des systèmes et services de soins de santé ou d'action sociale, sur la base d'une loi, à condition que le traitement soit effectué par ou sous la responsabilité d'un professionnel soumis à des obligations de confidentialité en vertu d'une loi ou de règles établies par des organismes nationaux compétents ; ou

- le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, sur la base d'une loi qui prévoit des mesures appropriées et spécifiques pour protéger les droits et libertés des personnes concernées, notamment le secret professionnel ; ou

- le traitement est nécessaire à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, sur la base d'une loi qui doit être proportionnée à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques visant à sauvegarder les droits fondamentaux et les intérêts de la personne concernée.

Règle 1D – Les Membres du Groupe évalueront l'impact de tout traitement de données à caractère personnel qui comportera des risques élevés pour les droits et libertés des personnes concernées.

Les Entités exportatrices, lorsqu'elles agissent en tant que responsables du traitement, évalueront la nécessité et la proportionnalité de tout nouveau traitement de données à caractère personnel et, dans le cas où celui-ci comporte des risques élevés pour les droits et libertés des personnes concernées, elles réaliseront une analyse d'impact relative à la protection des données conformément à la Législation européenne en matière de protection de données. Dans le cas où l'analyse d'impact relative à la protection des données indique que le traitement entraînera un risque élevé pour les personnes concernées, les Entités exportatrices seront tenues de consulter les autorités de contrôle compétentes, en l'absence de mesures prises pour atténuer le risque, avant de commencer le traitement.

RÈGLE 2 – GARANTIR LA TRANSPARENCE ET NE TRAITER LES DONNÉES À CARACTÈRE PERSONNEL QUE POUR UNE FINALITÉ CONNUE

Règle 2A – Les Membres du Groupe informeront les personnes concernées de la manière dont leurs données seront traitées.

Les Membres du Groupe veilleront à ce que les personnes concernées soient toujours informées de manière claire et complète (généralement au moyen d'une déclaration d'information loyale) de la manière dont leurs données à caractère personnel seront traitées. Le Membre du Groupe concerné fournira des informations conformes à ce qu'exige la Législation européenne en matière de protection de données, lesquelles incluront au minimum ce qui suit :

- l'identité et les coordonnées du responsable du traitement, y compris les coordonnées du délégué à la protection des données et du représentant, le cas échéant ;

- la finalité et la base juridique du traitement, y compris une explication concernant tout traitement fondé sur l'intérêt légitime et toute finalité compatible nouvelle ou différente ;

- les destinataires ou les catégories de destinataires des données à caractère personnel ;

- des informations sur les garanties mises en place pour protéger les données à caractère personnel lorsqu'elles sont transférées à l'international, ainsi que sur la manière d'accéder à ces garanties ou d'en obtenir une copie. Dans le cas de transferts de données à caractère personnel entre une Entité exportatrice et une Entité importatrice effectués sur la base de la présente Politique, les informations fournies comprendront une référence à la présente Politique et la manière d'y accéder ;

- la durée pendant laquelle les données à caractère personnel seront conservées ou les critères utilisés pour déterminer cette durée ;

- des informations sur les droits des personnes concernées, y compris le droit d'accès, le droit de rectification, le droit à l'effacement, le droit à la limitation du traitement, le droit d'opposition, le droit à la portabilité des données, le droit de retirer son consentement (lorsque le traitement est fondé sur le consentement) et le droit d'introduire une réclamation auprès d'une autorité de contrôle ;

- si la fourniture des informations constitue une obligation légale ou contractuelle, et les conséquences du défaut de fourniture de données à caractère personnel dans de telles circonstances ; et

- des informations sur l'existence d'une prise de décision automatisée, y compris le profilage, et, au moins dans les cas où de telles décisions produisent des effets juridiques pour la personne concernée ou l'affectent de manière similaire et significative, ou sont fondées sur des catégories particulières de données à caractère personnel, des informations pertinentes sur la logique sous-jacente, ainsi que sur l'importance et les conséquences envisagées d'un tel traitement pour la personne concernée.

La Législation locale en matière de PD applicable dans la juridiction où les données à caractère personnel sont collectées déterminera si des informations supplémentaires doivent être fournies aux personnes concernées.

Cette information sera fournie au moment où des données à caractère personnel sont obtenues par les Membres du Groupe auprès de la personne concernée ou dans un délai autrement autorisé par la Législation européenne en matière de protection de données.

Lorsque les Membres du Groupe obtiennent les données à caractère personnel de la personne concernée auprès d'une source autre que la personne concernée elle-même, le Membre du Groupe concerné fournira ces informations à la personne concernée, ainsi que des informations sur la source et les catégories de données à caractère personnel reçues de tiers, comme suit :

- dans un délai raisonnable après la collecte des données à caractère personnel, mais au plus tard dans un délai d'un (1) mois ;

- si les données à caractère personnel doivent être traitées aux fins de communication avec la personne concernée, au plus tard au moment de la première communication à cette personne concernée ; ou

- si elles doivent être communiquées à un tiers, au plus tard au moment de leur première communication.

Les Membres du Groupe respecteront la Règle 2A, sauf si le fait de ne pas fournir d'informations est expressément autorisé en vertu de la Législation européenne en matière de protection de données.

Règle 2B – Les Membres du Groupe ne collecteront et ne traiteront des données à caractère personnel que pour les finalités qui sont connues de la personne concernée, ou qui sont compatibles avec ses attentes et sont pertinentes pour les Membres du Groupe.

La Règle 1A prévoit que les Membres du Groupe se conformeront à toute législation applicable relative au traitement des données à caractère personnel (pour autant que ladite législation soit conforme aux exigences prévues par la Règle 13 ci-après, le cas échéant). Cela signifie que les Membres du Groupe collecteront des données à caractère personnel pour des finalités spécifiques, explicites et légitimes et ne traiteront pas ultérieurement ces données à caractère personnel d'une manière incompatible avec ces finalités.

Les Membres du Groupe identifieront et feront connaître les finalités pour lesquelles les données à caractère personnel seront traitées (y compris les utilisations secondaires et les communication des données), conformément à la Règle 2A.

Règle 2C – Les Membres du Groupe ne peuvent traiter les données à caractère personnel pour une finalité différente ou nouvelle que si cette finalité est compatible avec la finalité pour laquelle les données ont été collectées.

Si un Membre du Groupe collecte des données à caractère personnel à des fins déterminées conformément à la Règle 2A (telles que communiquées à la personne concernée via la notice d'information pertinente) et comme décrit dans la Règle 2B, et que, par la suite, le Membre du Groupe souhaite traiter des données à caractère personnel pour une finalité différente ou nouvelle, il ne traitera pas ultérieurement ces données d'une manière incompatible avec la finalité pour laquelle elles ont été collectées, sauf si ce traitement ultérieur est fondé sur le consentement de la personne concernée ou requis par la loi (pour autant que cette loi respecte les exigences prévues à la Règle 13 ci-après, le cas échéant).

RÈGLE 3 – ASSURER LA QUALITÉ DES DONNÉES

Règle 3A – Les Membres du Groupe maintiendront les données à caractère personnel exactes et mises à jour.

Afin de garantir que les données à caractère personnel détenues par les Membres du Groupe sont exactes et à jour, les Membres du Groupe encouragent activement les personnes concernées à les informer lorsque leurs données à caractère personnel sont modifiées. Les Membres du Groupe prendront toutes les mesures raisonnables pour veiller à ce que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

Règle 3B – Les Membres du Groupe ne conserveront les données à caractère personnel que pendant la durée nécessaire aux fins pour lesquelles elles sont traitées.

Les Membres du Groupe se conformeront à la réglementation applicable à chaque Membre du Groupe ainsi qu'aux politiques et procédures de conservation des documents du Groupe Santander telles que révisées et mises à jour de temps à autre. Cela signifie, entre autres, que les Membres du Groupe suppriment ou bloquent, selon le cas, les données à caractère personnel qui ne sont plus nécessaires aux fins pour lesquelles elles sont collectées et traitées ultérieurement.

Règle 3C – Les Membres du Groupe ne traiteront que les données à caractère personnel qui sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Les Membres du Groupe ne traiteront que les données à caractère personnel nécessaires à la bonne réalisation des finalités pour lesquelles elles sont traitées.

RÈGLE 4 – ADOPTION DE MESURES DE SÉCURITÉ APPROPRIÉES

Règle 4A – Les Membres du Groupe se conformeront aux politiques de sécurité informatique du Groupe Santander.

Les Membres du Groupe mettront en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction ou la perte accidentelles ou illicites, l'altération, la divulgation ou l'accès non autorisés, en particulier lorsque le traitement implique la transmission de données à caractère personnel sur un réseau, ainsi que contre toutes les autres formes de traitement illicites. À cette fin, les Membres du Groupe se conformeront aux exigences des politiques de sécurité en vigueur au sein du Groupe Santander, telles que révisées et mises à jour de temps à autre, ainsi qu'à toute autre procédure de sécurité pertinente pour un domaine d'activité ou une fonction. Compte tenu de l'état de la technique et des coûts de leur mise en œuvre, ces mesures doivent assurer un niveau de sécurité approprié aux risques présentés par le traitement et à la nature des données à protéger.

Règle 4B – Les Membres du Groupe ont mis en œuvre une politique de notification des violations de données.

Les Membres du Groupe ont mis en œuvre des procédures de réponse aux violations de données à caractère personnel (telles que révisées et mises à jour de temps à autre) qui définissent la procédure à suivre en cas de violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données (une « **Violation de données à caractère personnel** »).

En particulier, en cas de Violation de données à caractère personnel, la personne qui prend connaissance de la violation au sein du Membre du Groupe concerné la notifiera, sans retard indu, aux instances suivantes :

- au DPD ou au Champion concerné, par l'intermédiaire de la Fonction de contrôle du risque opérationnel (le cas échéant) ;
- au Membre du Groupe agissant en tant que responsable du traitement lorsque le Membre du Groupe concerné agit en tant que sous-traitant ; et
- au Membre soumis aux REC responsable.

Le DPD ou le Champion concerné évaluera, avec l'aide du Service corporatif de PD, le cas échéant, si la Violation de données à caractère personnel doit être notifiée à l'autorité de contrôle compétente. Si tel est le cas, le DPD ou, le cas échéant, le Champion concerné procédera à la notification d'une Violation de données à caractère personnel à l'autorité de contrôle compétente dans les délais requis (conformément á la Législation

européenne en matière de protection de données, sans retard injustifié et, si possible, 72 heures au plus tard après en avoir pris connaissance).

Les personnes concernées seront également informées sans retard injustifié dans les cas où la Violation de données à caractère personnel est susceptible d'entraîner un risque élevé pour leurs droits et libertés, sauf si une telle notification n'est pas requise en vertu de la Législation européenne en matière de protection de données.

Conformément à ce qui précède, les Violations de données à caractère personnel subies par les Membres du Groupe, comprenant les faits, les effets de tels incidents et les mesures correctives prises, seront également enregistrées dans Heracles, le registre des incidents de sécurité (y compris les Violations de données à caractère personnel) du Groupe Santander, qui sera mis à la disposition de l'autorité de contrôle compétente sur demande.

Règle 4C – Les Membres du Groupe veilleront à ce que les prestataires de services et les autres entités traitant des données à caractère personnel en leur nom adoptent également des mesures de sécurité appropriées et équivalentes.

Les Membres du Groupe qui recourent à un prestataire de services (agissant en qualité de sous-traitant) ayant accès aux données à caractère personnel des personnes concernées (par exemple, un prestataire de services de paie), doivent imposer par écrit au sous-traitant des obligations contractuelles conformes aux exigences de la Législation européenne en matière de protection de données, sous la forme d'un contrat de traitement des données contraignant. Ce contrat devra au minimum prévoir ce qui suit :

- l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées ;
- les obligations et les droits du responsable du traitement ;
- les obligations suivantes pour l'entité agissant en qualité de sous-traitant :
    - traiter les données à caractère personnel uniquement sur instructions documentées du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale, à moins que le droit auquel le sous-traitant est soumis ne l'y oblige (pour autant que ledit droit soit conforme aux exigences prévues à la Règle 13 ci-après, le cas échéant). Dans un tel cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si cette loi interdit une telle information pour des motifs importants d'intérêt public ;
    - veiller à ce que les personnes autorisées à traiter les données à caractère personnel se soient engagées à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
    - mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque lié au traitement des données à caractère personnel ;
    - ne pas engager un autre sous-traitant en relation avec les données à caractère personnel sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement et, le cas échéant, conclure un contrat écrit avec le sous-traitant ultérieur imposant à ce dernier les mêmes obligations en matière de protection des données que celles énoncées dans le contrat ou tout autre acte juridique conclu entre le responsable du traitement et le sous-traitant

(prévoyant notamment des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la Législation européenne en matière de protection de données) ;

- compte tenu de la nature du traitement, aider le responsable du traitement, au moyen de mesures techniques et organisationnelles appropriées, dans la mesure du possible, afin de lui permettre de s'acquitter de son obligation de répondre aux demandes d'exercice des droits de la personne concernée (telles que décrites plus en détail dans la Règle 5 ci-dessous) ;

- aider le responsable du traitement à veiller au respect des obligations relatives à la mise en œuvre de mesures de sécurité appropriées, à la réalisation d'analyses d'impact relatives à la protection des données et aux consultations connexes auprès des autorités de contrôle compétentes ; ainsi que des obligations de notification des Violations de données à caractère personnel aux autorités de contrôle compétentes et aux personnes concernées (le cas échéant) ;

- au choix du responsable du traitement, supprimer ou renvoyer toutes les données à caractère personnel au responsable du traitement à l'issue de la fourniture des services relatifs au traitement, et supprimer les copies existantes à moins que la loi n'exige la conservation des données à caractère personnel ;

- mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations incombant au sous-traitant et pour permettre et contribuer aux audits, y compris aux inspections, réalisés par le responsable du traitement ou par un autre auditeur mandaté par le responsable du traitement ; et

- informer immédiatement le responsable du traitement s'il estime qu'une instruction enfreint la loi.

RÈGLE 5 – RESPECT DES DROITS DES PERSONNES CONCERNÉES

Règle 5 – Les Membres du Groupe traiteront les demandes relatives aux droits des personnes concernées en matière de protection des données (y compris celles portant sur l'accès, la rectification, l'effacement, la limitation du traitement ou la portabilité des données à caractère personnel, ainsi que les oppositions au traitement des données à caractère personnel et le retrait du consentement).

Sur demande, les personnes concernées sont en droit de demander l'exercice des droits suivants, conformément à la Législation européenne en matière de protection des données :

- droit d'accès, ce qui implique de fournir des informations sur les données à caractère personnel disponibles sur la personne concernée et confirmer si les données à caractère personnel de la personne concernée sont traitées ;

- droit de rectification, en vertu duquel la personne concernée a le droit d'obtenir la rectification de toute donnée à caractère personnel susceptible d'être inexacte ou incomplète ;

- droit à l'effacement ou « droit à l'oubli », en vertu duquel la personne concernée a le droit d'obtenir l'effacement de ses données à caractère personnel lorsque certaines conditions sont réunies (telles que celles prévues à l'article 17 du RGPD) ;

- droit à la limitation du traitement, en vertu duquel la personne concernée a le droit de demander la limitation du traitement de ses données à caractère personnel dans certaines circonstances (telles que celles prévues à l'article 18 du RGPD) ;

- droit d'obtenir que chaque destinataire auquel les données à caractère personnel ont été communiquées soit informé de toute rectification ou de tout effacement de données à caractère personnel ou de toute limitation du traitement, à moins que cela ne s'avère impossible ou n'implique des efforts disproportionnés. La personne concernée peut également demander à être informée desdits destinataires ;

- droit à la portabilité des données, en vertu duquel la personne concernée a le droit de recevoir les données à caractère personnel la concernant, qu'elle a fournies à un responsable du traitement, dans un format structuré, et de les transmettre à un autre responsable du traitement ;

- droit d'opposition, en vertu duquel la personne concernée a le droit de s'opposer au traitement de ses données à caractère personnel pour une finalité spécifique, y compris au traitement à des fins de prospection commerciale directe et au profilage, dans la mesure où ce dernier est lié à une telle prospection ;

- droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques le concernant ou l'affectant de manière significative (le cas échéant) ; et

- droit de retirer à tout moment le consentement donné pour un traitement spécifique.

RÈGLE 6 – GARANTIR UNE PROTECTION ADÉQUATE DES TRANSFERTS ET DES TRANSFERTS ULTÉRIEURS

Règle 6 – Les Membres du Groupe ne transféreront pas de données à caractère personnel à des tiers en dehors de l'Europe sans garantir une protection adéquate pour les données à caractère personnel conformément aux normes énoncées dans la présente Politique et à la Législation européenne en matière de protection de données.

Les transferts et les transferts ultérieurs de données à caractère personnel provenant de Membres du Groupe soumis à la Législation européenne en matière de protection de données à des tiers situés en dehors de l'Europe ne sont pas autorisés sans la mise en œuvre de mesures appropriées, comme l'exige la Législation européenne en matière de protection de données.

Ces mesures peuvent inclure, entre autres, les suivantes :

- confirmer que le tiers est établi dans un pays que la Commission européenne a considéré comme assurant un niveau de protection adéquat pour les données à caractère personnel transférées ; ou

- conclure de clauses contractuelles types appropriées ou d'autres mécanismes prévus par la Législation européenne en matière de protection de données ; ou

- assurer que le transfert est nécessaire pour : (i) l'exécution d'un contrat entre la personne concernée et le Membre du Groupe effectuant le transfert ou pour la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ; (ii) la conclusion ou l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le Membre du Groupe effectuant le transfert et une autre partie ; (iii) des motifs importants d'intérêt public reconnus par le Droit de l'Union ou par le Droit de l'État membre auquel le responsable du traitement est soumis ; (iv) la

constatation, l'exercice ou la défense de droits en justice ; (v) la protection des intérêts vitaux de la personne concernée ou d'une autre personne physique et lorsque la personne concernée est dans l'incapacité de donner son consentement ; ou (vi) l'obtention du consentement explicite des personnes concernées, après que ces personnes concernées ont été informées des risques éventuels d'un tel transfert en raison de l'absence d'une décision d'adéquation et de garanties appropriées.

SECTION B : ENGAGEMENTS PRATIQUES

RÈGLE 7 – CONFORMITÉ ET RESPONSABILITÉ

Règle 7A – Les Membres du Groupe seront responsables de la conformité à la présente Politique et seront en mesure d'en démontrer le respect et disposeront de personnel et de soutien appropriés pour assurer et superviser la conformité à la présente Politique dans l'ensemble de l'entreprise.

Le Groupe Santander dispose d'une structure organisationnelle en matière de protection de la vie privée chargée de décider, de coordonner, de mettre en œuvre et de superviser tout événement susceptible de se produire au sein du Groupe Santander en matière de protection des données (l'« **Équipe de protection de la vie privée** »). La structure de protection des données du Groupe Santander est composée de ce qui suit :

- **Service corporatif de protection des données** (« **Service corporatif de PD** ») : Instance de l'entreprise chargée de définir les critères généraux et d'élaborer les politiques de protection des données applicables au sein de l'entreprise. Il est constitué, avec l'équipe des Risques non financiers, en tant que deuxième ligne de défense (2LoD) mondiale, chargée de superviser la gestion des activités liées à la protection de la vie privée menées par la première ligne de défense (1LoD) et de veiller à une gestion adéquate des risques conformément à la propension au risque du Groupe Santander.

  En tant que 2LoD mondiale, le Service corporatif de PD et l'équipe des Risques non financiers exercent une série de fonctions pour l'ensemble des entités du Groupe Santander soumises à la Législation européenne en matière de protection de données, notamment :

  - surveillance et contrôle de la conformité : (i) supervision de la conformité du Groupe Santander en matière de protection des données ; (ii) *reporting* consolidé à la haute direction du Groupe Santander ; (iii) point de contact mondial, par l'intermédiaire des différents DPD locaux (ou fonction similaire), avec les autorités de contrôle compétentes ; (iv) analyse de l'impact, conjointement avec les fonctions métiers et de support concernées, des incidents de sécurité à l'échelle mondiale ; (v) analyse et *reporting* mondiaux des risques en matière de protection des données ; et (vi) faciliter la mise en œuvre des critères du Groupe et servir de point de contact au sein du Groupe pour les DPD/Champions des entités (voir ci-dessous).

  - Fonction de soutien auprès des DPD et des Champions du groupe Santander (unités/entité(s) *corporate* et entités locales). Fournir principalement des conseils spécialisés en matière de réglementation, ainsi qu'un soutien à la mise en œuvre des fonctions locales de protection des données personnelles.

- **Structure et gouvernance**

  - **Banco Santander (Corporation)** : deux acteurs clés apportent leur soutien et rendent compte au Service corporatif de PD :

- **le DPD de Banco Santander** (formellement nommé auprès de l'autorité de contrôle espagnole) : ses fonctions au sein de la société mère, que le DPD exerce de manière indépendante, se limitent à celles décrites dans le RGPD qui requièrent notamment sa participation au dialogue avec l'autorité de contrôle espagnole. Sans préjudice des obligations de *reporting* et d'assistance du DPD envers le Service corporatif de PD, le DPD rend compte directement au plus haut niveau de la direction de Banco Santander.

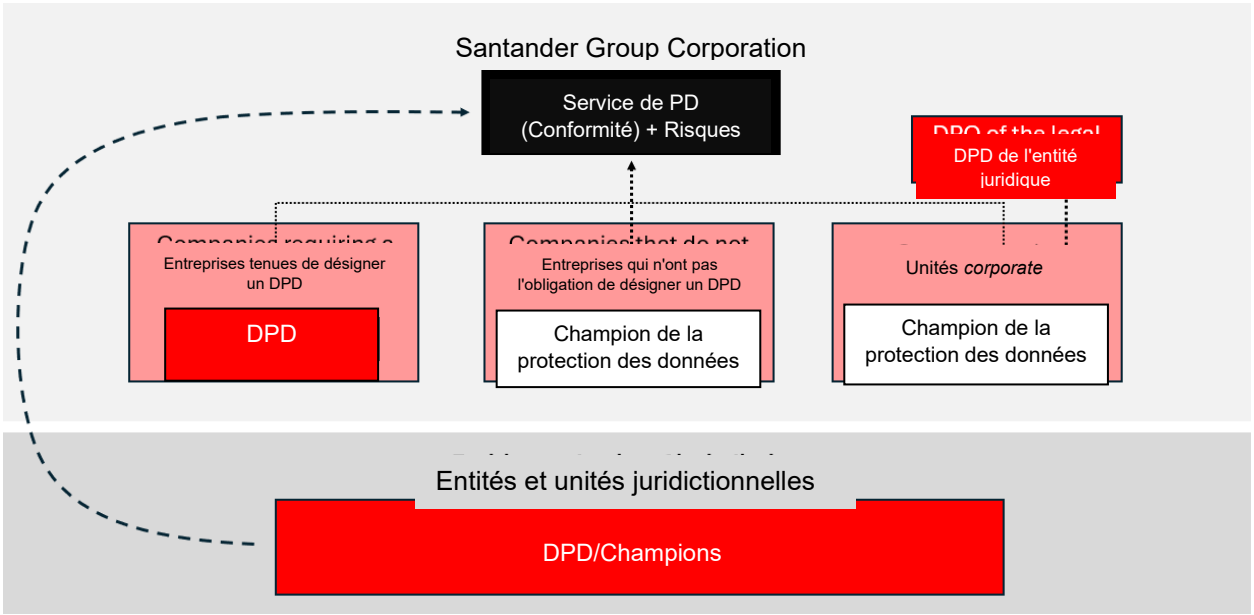
- **Unités *corporate*** : unités désignées dans l'ensemble de l'organisation. Leurs principaux rôles et responsabilités sont les suivants : (a) traiter et résoudre en première instance les questions relatives aux données à caractère personnel ; (b) informer et conseiller les responsables du traitement, les sous-traitants et les employés sur la manière de se conformer à la réglementation applicable en matière de protection des données ; (c) surveiller le respect de la réglementation en matière de protection des données ; (d) assurer le rôle de point de contact interne en tant que fonction de support de premier niveau ; (e) canaliser les questions et les demandes d'assistance vers le Service corporatif de PD et assurer le *reporting* des indicateurs de gestion.

- **Unités locales** : il existe également deux rôles qui relèvent du Service corporatif de PD :

  - **DPD (ou fonction locale équivalente)** : lorsque la Législation locale en matière de PD applicable l'exige, un DPD (ou une fonction locale équivalente) est désigné. Ses principaux rôles et responsabilités peuvent inclure les suivants : (a) point de contact avec l'autorité de contrôle compétente et avec les parties prenantes ; (b) coopération avec l'autorité de contrôle compétente ; (c) conseils en matière de protection des données ; (d) suivi et supervision ; (e) formation ; (f) conseils sur les analyses d'impact relatives à la protection des données ; (g) réalisation de consultations préalables avec l'autorité de contrôle compétente ; (h) supervision du registre des activités de traitement ; (i) conseils sur la notification des Violations de données à caractère personnel ; (j) conseils sur la gestion des tiers ; et (k) supervision de l'exercice des droits des personnes concernées.

  - **Champions ou figure locale similaire (par exemple, responsable de la protection de la vie privée)** : lorsqu'aucun DPD n'est requis au titre de la Législation locale en matière de PD applicable ou lorsque, en raison de la taille et/ou de la complexité d'une entité, il est nécessaire de disposer d'un grand nombre de DPD ou de fonctions locales similaires, le Service corporatif de PD peut être soutenu par et recevoir des rapports de la part de Champions locaux ou d'une figure similaire (par exemple, responsable de la protection de la vie privée). Leur rôle et leurs responsabilités sont très similaires à ceux des DPD ou d'une fonction similaire, à l'exception des communications avec les autorités de contrôle (auxquelles ils ne participent pas).

Vous trouverez ci-dessous un schéma présentant la structure organisationnelle et relationnelle entre les acteurs susmentionnés responsables de la protection des données au sein du Groupe Santander :



Règle 7B – Les Membres du Groupe mettront en œuvre des mesures techniques et organisationnelles appropriées, dès la conception et par défaut, afin de permettre et de faciliter la conformité à la Politique dans la pratique.

Compte tenu de l'état de l'art et du coût de mise en œuvre, ainsi que de la portée, de la nature, du contexte et des finalités du traitement, les Membres du Groupe mettront en œuvre des mesures techniques et organisationnelles appropriées, conformes aux principes de protection des données dès la conception et par défaut, comme l'exige la Législation européenne en matière de protection des données. Les Membres du Groupe intégreront de telles mesures au traitement lors de la détermination des moyens du traitement, ainsi qu'au moment du traitement lui-même, afin de faciliter la protection des données à caractère personnel traitées et de veiller à ce que, par défaut, seules les données à caractère personnel nécessaires à chaque finalité spécifique du traitement soient traitées.

Règle 7C – Les Membres du Groupe traitant des données à caractère personnel tiendront un registre écrit (y compris sous forme électronique) de leurs activités de traitement et mettront ce registre à la disposition des autorités de contrôle compétentes sur demande.

Les registres des activités de traitement tenus par les Membres du Groupe, agissant en tant que responsables du traitement, contiendront :

- le nom et les coordonnées du Membre du Groupe et, le cas échéant, le responsable conjoint du traitement, le représentant du responsable du traitement et le délégué à la protection des données ;
- les finalités pour lesquelles les données à caractère personnel sont traitées ;
- une description des catégories de personnes concernées dont les données à caractère personnel sont traitées et des données à caractère personnel traitées ;
- les catégories de destinataires auxquels des données à caractère personnel ont été ou seront communiquées y compris les destinataires dans des pays tiers ou des organisations internationales ;

- détails du ou des pays tiers vers lesquels des données à caractère personnel sont transférées, y compris l'identification de ce pays tiers ou de cette organisation internationale et la documentation des garanties appropriées mises en œuvre pour légitimer de tels transferts (sauf si le pays a été déclaré adéquat au titre de la Législation européenne en matière de protection de données) ;

- dans la mesure du possible, la durée pendant laquelle les données à caractère personnel seront conservées ; et

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles utilisées pour protéger les données à caractère personnel.

Les registres des activités de traitement tenus par les Membres du Groupe, agissant en tant que sous-traitants pour le compte d'un Membre du Groupe qui est le responsable du traitement, comprendront :

- le nom et les coordonnées du membre du groupe et de chaque responsable du traitement pour le compte duquel le sous-traitant agit, et, le cas échéant, du représentant du responsable du traitement ou du sous-traitant, et du délégué à la protection des données ;

- les catégories d'activités de traitement effectuées pour le compte de chaque responsable du traitement ;

- détails du ou des pays tiers vers lesquels des données à caractère personnel sont transférées, y compris l'identification de ce pays tiers ou de cette organisation internationale et la documentation des garanties appropriées mises en œuvre pour légitimer de tels transferts (sauf si le pays a été déclaré adéquat au titre de la Législation européenne en matière de protection de données) ; et

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles utilisées pour protéger les données à caractère personnel.

Les registres des activités de traitement tenus par les Membres du Groupe sont établis par écrit, y compris en format électronique, et seront mis à la disposition des autorités de contrôle compétentes sur demande.

RÈGLE 8 – FORMATION

Règle 8 – Les Membres du Groupe fourniront une formation appropriée aux employés qui ont un accès permanent ou régulier aux données à caractère personnel et/ou qui participent au traitement de données à caractère personnel ou au développement d'outils utilisés pour traiter ces données à caractère personnel.

Les Membres du Groupe fourniront une formation appropriée et à jour aux employés qui ont un accès permanent ou régulier aux données à caractère personnel et/ou qui participent au traitement de ces données à caractère personnel ou au développement d'outils utilisés pour traiter ces données à caractère personnel. Une telle formation sera dispensée au moins une fois tous les deux ans et portera, entre autres, sur les procédures de gestion des demandes d'accès aux données à caractère personnel émanant des autorités publiques.

RÈGLE 9 – AUDIT

Règle 9 – Les Membres du Groupe se conformeront au Programme d'audit prévu à l'Annexe 1.

Les Membres du Groupe se conformeront au Programme d'audit en effectuant des audits internes réguliers et en autorisant, le cas échéant, des audits externes, conformément au processus d'évaluation formel tel que stipulé dans le Programme d'audit. Les résultats de tels audits seront communiqués conformément à l'Annexe 1.

RÈGLE 10– TRAITEMENT DES RÉCLAMATIONS

Règle 10 – Les Membres du Groupe respecteront la Procédure de traitement des réclamations énoncée dans l'Annexe 2.

Les Membres du Groupe se conformeront à la Procédure de traitement des réclamations telle qu'énoncée dans l'Annexe 2 afin de traiter de manière adéquate les réclamations des personnes concernées et de garantir la protection des données à caractère personnel traitées par les Membres du Groupe. Les Membres du Groupe permettront également l'exercice des droits des tiers bénéficiaires tels qu'énoncés dans la section C de la présente Politique.

RÈGLE 11 – COOPÉRATION AVEC LES AUTORITÉS DE CONTRÔLE COMPÉTENTES

Règle 11 – Les Membres du Groupe se conformeront à la Procédure de coopération prévue à l'Annexe 3.

Les Membres du Groupe se conformeront à la Procédure de coopération énoncée dans l'Annexe 3 et coopéreront avec les autorités de contrôle compétentes en lien avec la présente Politique, accepteront de faire l'objet d'un audit et d'être inspectés par celles-ci (y compris, si nécessaire, sur site), et tiendront compte de leurs avis et se conformeront à leurs décisions sur toute question liée à la présente Politique.

RÈGLE 12 – MISE À JOUR DES RÈGLES

Règle 12 – Les Membres du Groupe se conformeront à la Procédure de mise à jour énoncée dans l'Annexe 4.

Les Membres du Groupe se conformeront à la Procédure de mise à jour prévue à Annexe 4 et communiqueront sans retard injustifié toute mise à jour de la présente Politique et de la liste des Membres du Groupe aux autorités de contrôle compétentes, aux personnes concernées et aux Membres du Groupe, le cas échéant.

RÈGLE 13 – MESURES À ADOPTER DANS LES CAS OÙ LA LÉGISLATION NATIONALE ENTRAVE LA CONFORMITÉ AVEC LA POLITIQUE

Règle 13A – Les Membres du Groupe s'engagent à n'utiliser la présente Politique qu'en tant qu'outil pour les transferts vers des Entités importatrices pour lesquelles ils ont dûment évalué que la législation et les pratiques du pays des Entités importatrices (y compris toute exigence de communication de données à caractère personnel ou toute mesure autorisant l'accès par les autorités publiques) ne les empêchent pas de s'acquitter de leurs obligations au titre de la présente Politique.

Les Membres du Groupe n'utiliseront la présente Politique comme outil pour sécuriser les transferts internationaux que lorsqu'ils auront évalué que le droit et les pratiques en vigueur dans les pays tiers de destination concernés, y compris toute exigence de communication de données à caractère personnel ou toute mesure autorisant l'accès par les autorités publiques, ne les empêchent pas de s'acquitter de leurs obligations au titre de la présente Politique. Cela reposera sur le principe selon lequel les lois et pratiques qui respectent

l'essence des droits et libertés fondamentaux et ne dépassent pas ce qui est nécessaire et proportionné dans une société démocratique ne sont pas contraires à la Politique.

Lors de l'évaluation des lois et pratiques des pays tiers susceptibles d'entraver le respect des engagements contenus dans la présente Politique, les Membres du Groupe doivent dûment tenir compte, en particulier, des éléments suivants :

(i) les circonstances spécifiques du transfert ou de la série de transferts, et de tout transfert ultérieur envisagé au sein du même pays tiers ou vers un autre pays tiers, y compris :

- finalités pour lesquelles les données sont transférées et traitées (par exemple, marketing, RH, conservation, support informatique, etc.) ;
- types d'entités impliquées dans le traitement (l'Entité importatrice et tout autre destinataire de tout transfert ultérieur) ;
- secteur économique concerné par le transfert ou l'ensemble des transferts ;
- catégories et format des données à caractère personnel transférées ;
- lieu du traitement, y compris la conservation ; et
- canaux de transmission utilisés.

(ii) les lois et pratiques des pays tiers de destination pertinentes à la lumière des circonstances du transfert. Celles-ci peuvent inclure : (a) celles exigeant la communication de données aux autorités publiques ou autorisant l'accès par ces autorités ; (b) celles prévoyant l'accès à ces données pendant le transit entre les pays des Entités exportatrices et ceux des Entités importatrices ; et (c) les limitations et garanties applicables.

(iii) toutes garanties contractuelles, techniques ou organisationnelles pertinentes mises en place pour compléter les garanties prévues par la présente Politique. Cela comprend des mesures appliquées lors de la transmission et au traitement des données à caractère personnel dans les pays de destination.

Dans les cas où des garanties supplémentaires, en plus de celles prévues par la présente Politique, doivent être mises en place, le Membre soumis aux REC responsable ainsi que le DPD ou le Champion concerné, selon le cas, doivent être informés et associés à l'évaluation. Les Membres du Groupe doivent documenter de manière appropriée cette évaluation, ainsi que les mesures supplémentaires choisies et mises en œuvre. Ils mettent cette documentation à la disposition de l'autorité de contrôle compétente sur demande.

Les Entités importatrices doivent notifier sans délai les Entités exportatrices si, lorsqu'elles utilisent la présente Politique comme outil de transfert, et pendant toute la durée de l'adhésion, elles ont des raisons de croire qu'elles sont soumises ou elles ont passé à être soumises à des lois ou à des pratiques qui les empêcheraient de s'acquitter de leurs obligations en vertu de la présente Politique. Cela comprend l'impossibilité de remplir ses obligations à la suite d'une modification de la législation du pays tiers concerné ou d'une mesure (telle qu'une demande de communication). Ces informations devraient également être fournies au Membre soumis aux REC responsable.

Après vérification d'une telle notification, l'Entité exportatrice concernée, ainsi que le Membre soumis aux REC responsable et le DPD ou le Champion concerné, selon le cas, s'engagent à identifier sans délai des mesures supplémentaires (par exemple, des mesures techniques ou organisationnelles visant à garantir la sécurité et la confidentialité) à adopter par l'Entité exportatrice et/ou l'Entité importatrice afin de leur permettre de s'acquitter de leurs obligations au titre de la présente Politique. Il en va de même si une Entité exportatrice a

des raisons de croire qu'une Entité importatrice ne peut plus s'acquitter de ses obligations au titre de la présente Politique.

Lorsque l'entité exportatrice concernée, de concert avec le Membre soumis aux REC responsable et le DPD ou le Champion concernés, selon le cas, estime que la Politique –même assortie de mesures supplémentaires– ne peut pas être respectée pour un transfert ou un ensemble de transferts, ou sur instruction de l'autorité de contrôle compétente, elle s'engage à suspendre le transfert ou l'ensemble de transferts en cause, ainsi que tous les transferts pour lesquels la même évaluation et le même raisonnement conduiraient à un résultat similaire, jusqu'à ce que la conformité soit à nouveau garantie ou que le transfert prenne fin.

À la suite d'une telle suspension, l'Entité exportatrice doit mettre fin au transfert ou à l'ensemble des transferts si la présente Politique ne peut pas être respectée et que la conformité n'est pas rétablie dans un délai d'un mois à compter de la suspension. Dans ce cas, les données à caractère personnel qui ont été transférées avant la suspension, ainsi que toutes les copies qui en ont été faites, doivent, au choix de l'Entité exportatrice, être restituées ou détruites dans leur intégralité.

Le Membre soumis aux REC responsable et, le cas échéant, le DPD ou le Champion concerné, informeront tous les autres Membres du Groupe de l'évaluation réalisée et de ses résultats, de sorte que les mesures supplémentaires identifiées soient appliquées si le même type de transferts est effectué par tout autre Membre du Groupe ou, si des mesures supplémentaires efficaces ne peuvent être mises en place, que les transferts en cause soient suspendus ou interrompus.

Les Entités exportatrices surveillent également de manière continue et, le cas échéant, en collaboration avec les Entités importatrices, les évolutions dans les pays tiers vers lesquels elles ont transféré des données à caractère personnel, susceptibles d'affecter l'évaluation initiale du niveau de protection et les décisions prises en conséquence concernant ces transferts.

Règle 13B – Les Entités importatrices veilleront à ce que, lorsqu'elles reçoivent, en vertu des lois du pays de destination, une demande juridiquement contraignante d'une autorité publique visant la communication de données à caractère personnel transférées conformément à la Politique, ou lorsqu'elles prennent connaissance, conformément aux lois du pays de destination, d'un accès direct par des autorités publiques aux données à caractère personnel transférées conformément à la Politique, elles en informent sans délai l'Entité exportatrice et, dans la mesure du possible, la personne concernée (si nécessaire avec l'aide de l'Entité exportatrice).

Les Entités importatrices notifieront sans délai l'Entité exportatrice concernée et, dans la mesure du possible, la personne concernée (si nécessaire, avec l'aide de l'Entité exportatrice) si elles :

- reçoivent une demande juridiquement contraignante, émanant d'une autorité publique en vertu des lois du pays de destination ou d'un autre pays tiers, aux fins de la communication de données à caractère personnel transférées conformément à la Politique (ladite notification doit inclure des informations concernant les données à caractère personnel demandées, l'autorité requérante, le fondement juridique de la demande et la réponse fournie) ; ou

- prennent connaissance de tout accès direct par les autorités publiques aux données à caractère personnel transférées en vertu de la Politique, conformément aux lois du pays de destination (ladite notification doit inclure toutes les informations dont dispose l'Entité importatrice).

Si l'Entité importatrice se voit interdire de notifier l'accès à l'Entité exportatrice et/ou à la personne concernée, elle déploiera tous ses efforts pour obtenir la levée de l'interdiction, en vue de communiquer à l'Entité

exportatrice autant d'informations que possible et dans les meilleurs délais, et documentera ses efforts afin de pouvoir les démontrer sur demande de l'Entité exportatrice.

L'Entité importatrice fournira à l'Entité exportatrice, à intervalles réguliers, autant d'informations pertinentes que possible sur les demandes reçues (notamment le nombre de demandes, le type de données demandé, l'autorité ou les autorités requérantes, si les demandes ont été contestées et l'issue de ces contestations, etc.). Si l'Entité importatrice est l'objet ou devient l'objet d'une interdiction, partielle ou total, de fournir à l'Entité exportatrice les informations susmentionnées, elle en informe l'Entité exportatrice sans délai indu.

L'Entité importatrice conservera les informations susmentionnées aussi longtemps que les données seront soumises aux garanties prévues par la Politique et les mettra à la disposition de l'autorité de contrôle compétente sur demande.

L'Entité importatrice examinera la légalité de la demande de divulgation, notamment si elle s'inscrit dans les limites des compétences conférées à l'autorité publique requérante, et contestera la demande si, après un examen attentif, elle conclut qu'il existe des motifs raisonnables de considérer que la demande est illicite au regard des lois du pays de destination, des obligations applicables en vertu du Droit international et des principes de courtoisie internationale. L'Entité importatrice est tenue, dans les mêmes conditions, d'exercer les voies de recours. Lorsqu'elle conteste une demande, l'Entité importatrice doit solliciter des mesures provisoires en vue de suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente ait statué sur le fond. Les données à caractère personnel demandées ne seront pas communiquées tant qu'une telle communication n'est pas requise par les règles de procédure applicables.

L'Entité importatrice documentera son évaluation juridique ainsi que toute contestation de la demande de divulgation et, dans la mesure permise par les lois du pays de destination, mettra ladite documentation à la disposition de l'Entité exportatrice. Elle la mettra également à la disposition de l'autorité de contrôle compétente sur demande.

L'Entité importatrice fournira le minimum d'informations autorisé lorsqu'elle répondra à une demande de communication, sur la base d'une interprétation raisonnable de la demande.

En tout état de cause, les Membres du Groupe veilleront à ce que les transferts de données à caractère personnel effectués en vertu de la présente Politique à destination d'une autorité publique ne soient pas massifs, disproportionnés ou indiscriminés d'une manière qui irait au-delà de ce qui est nécessaire dans une société démocratique.

RÈGLE 14 – NON-RESPECT DE LA POLITIQUE ET CESSATION

Règle 14A – Les Entités exportatrices ne transféreront des données à caractère personnel qu'aux Entités importatrices qui sont effectivement assujetties à la Politique et en mesure d'en assurer le respect.

Aucun transfert au titre de la présente Politique ne sera effectué à un Membre du Groupe, sauf si ce Membre du Groupe est effectivement lié par la Politique et est en mesure d'en garantir le respect. Lorsque une Entité importatrice est dans l'impossibilité de se conformer à la Politique, pour quelque raison que ce soit, elle en informe sans délai l'Entité exportatrice. En cas de manquement de l'Entité importatrice à la Politique ou d'impossibilité pour elle de s'y conformer, l'Entité exportatrice doit suspendre le transfert ou ne pas procéder à celui-ci.

L'Entité importatrice doit, au choix de l'Entité exportatrice, restituer ou supprimer immédiatement l'ensemble des données à caractère personnel transférées en vertu de la Politique, lorsque :

- l'Entité exportatrice a suspendu le transfert et le respect de la présente Politique n'est pas rétabli dans un délai raisonnable et, en tout état de cause, au plus tard dans le mois suivant la suspension ; ou

- l'Entité importatrice est en manquement substantiel ou persistant à la Politique ; ou

- l'Entité importatrice ne se conforme pas à une décision contraignante d'une juridiction compétente ou d'une autorité de contrôle compétente relative à ses obligations au titre de la Politique.

Il en est de même pour toutes les copies des données. L'Entité importatrice doit certifier à l'Entité exportatrice la suppression des données. Jusqu'à ce que les données soient supprimées ou restituées, l'Entité importatrice doit continuer d'assurer le respect de la Politique. Lorsqu'une interdiction légale empêche l'Entité importatrice de restituer ou de supprimer les données à caractère personnel transférées, l'Entité importatrice garantit qu'elle continuera à veiller au respect de la Politique et ne traitera les données que dans la mesure et pour la durée légalement requises.

Règle 14B – L'Entité importatrice qui cesse d'être liée par la Politique doit s'assurer que les données à caractère personnel sont, selon le cas, conservées de manière appropriée, restituées ou supprimées.

Une Entité importatrice qui cesse d'être liée par la Politique peut, selon le cas, conserver, restituer ou supprimer les données à caractère personnel reçues en vertu de la présente Politique. Si l'Entité exportatrice et l'Entité importatrice conviennent que les données peuvent être conservées par l'Entité importatrice, la protection prévue par les présentes doit être maintenue.

SECTION C : DROITS DES TIERS BÉNÉFICIAIRES

C.1 Les personnes concernées dont les données à caractère personnel sont transférées à une Entité importatrice doivent pouvoir bénéficier de certains droits en tant que tiers bénéficiaires. À cette fin, les personnes concernées peuvent exiger le respect de :

- Règles 1B et 1C de la Politique (relatives à la loyauté et à la licéité, ainsi qu'au traitement de catégories particulières de données à caractère personnel) ;

- Règle 2 de la Politique (relative à la transparence et le traitement des données à caractère personnel uniquement pour une finalité connue) ;

- Règle 3 de la Politique (relative à la minimisation des données, à l'exactitude et à des durées de conservation limitées) ;

- Règle 4 de la Politique (relative aux mesures de sécurité appropriées et les obligations de notification en cas de violation de données) ;

- Règle 5 de la Politique (relative au respect des droits des personnes concernées) ;

- Règle 6 de la Politique (relative à la protection adéquate des transferts et des transferts ultérieurs) ;

- Règle 10 de la Politique (relative à la gestion des réclamations) ;

- Règle 11 de la Politique (relative à la coopération avec les autorités de contrôle compétentes) ;

- Règle 12 de la Politique (relative à la mise à jour des règles) ;
- Règle 13 de la Politique (relative aux mesures à prendre lorsque la législation nationale empêche le respect de la Politique) ;
- les dispositions figurant dans les sections C1 à C3 accordant des droits aux tiers bénéficiaires et fixant les règles de responsabilité et de compétence au titre de la Politique ; et
- le droit d'accéder à la Politique disponible sur la page web, dans le réseau interne (accessible aux employés) de la société ou d'obtenir une copie papier de la Politique, ainsi qu'une liste des Membres du Groupe tenus par cette Politique.

en :

- *déposant une réclamation* : les personnes concernées peuvent introduire des réclamations auprès d'un Membre du Groupe (conformément à la Procédure de traitement des réclamations énoncée dans l'Annexe 2) et auprès de l'autorité de contrôle de l'État membre dans lequel la violation alléguée a eu lieu, ou dans lequel la personne concernée travaille ou réside habituellement ; et/ou
- *engageant une action* : les personnes concernées peuvent engager une action contre les Membres du Groupe devant les juridictions d'un État membre dans lequel le Membre du Groupe dispose d'un établissement, ou dans l'État membre dans lequel la personne concernée a sa résidence habituelle.

Comme précisé plus en détail aux Sections C.2 à C.4, lorsqu'un manquement est commis par un Membre du Groupe situé en dehors de l'EEE, les personnes concernées conservent le droit de déposer des réclamations auprès du Membre soumis aux REC responsable désigné et d'intenter des actions à son encontre, comme si le manquement avait été commis par cette entité dans l'État membre où elle est établie.

Ces droits ne s'étendent pas aux éléments de la Politique relatifs aux mécanismes internes mis en œuvre au sein des Membres du Groupe, tels que les détails relatifs à la formation, au programme d'audit, au réseau de conformité et au mécanisme de mise à jour desdits éléments.

En outre, les Membres du Groupe acceptent que les personnes concernées puissent être représentées par un organisme, une organisation ou une association à but non lucratif dans les conditions prévues à l'article 80, paragraphe 1, du RGPD.

C.2 Les personnes concernées peuvent également demander au Membre soumis aux REC responsable une réparation appropriée, et celui-ci s'engage à prendre les mesures nécessaires pour remédier à toute violation des dispositions énumérées à la sous-section C.1 par toute Entité importatrice et, le cas échéant, à indemniser les personnes concernées pour tout dommage (matériel ou immatériel) subi du fait d'une violation des dispositions ou de l'une d'entre elles énumérées à la sous-section C.1 par une Entité importatrice, conformément à la décision d'un tribunal ou d'une autre autorité compétente.

C.3 Pour éviter toute ambiguïté, les personnes concernées bénéficieront des droits de tiers bénéficiaires tels que décrits dans la présente section C, et les juridictions européennes ou les autorités de contrôle compétentes seront compétentes comme si la violation des dispositions décrites dans la présente section C, ou de l'une quelconque d'entre elles, avait été causée par le Membre soumis aux REC responsable.

C.4 En cas de réclamation dans laquelle une personne concernée a subi un dommage du fait d'une violation de la présente Politique, les Membres du Groupe ont convenu que la charge de la preuve visant à démontrer qu'une Entité importatrice n'est pas responsable de la violation, ou qu'aucune violation n'a eu lieu, incombera au Membre soumis aux REC responsable.

PARTIE III : ANNEXES

ANNEXE 1

PROGRAMME D'AUDIT

1. INTRODUCTION

1.1 Les Membres du Groupe sont tenus de procéder à un audit de leur conformité à la Politique et doivent satisfaire à certaines conditions à cet effet. Ce document décrit comment les Membres du Groupe traitent de telles exigences.

1.2 Les *activités habituelles* (BAU) des DPD et des Champions comprennent la fourniture de conseils concernant le traitement de données à caractère personnel soumis à la Politique et l'évaluation des traitements de données à caractère personnel effectués par les Membres du Groupe afin d'identifier les risques potentiels liés à la protection de la vie privée dans le cadre des activités quotidiennes. Le traitement des données à caractère personnel est donc soumis à un examen et une évaluation approfondis de manière continue.

1.3 En tant que 2LoD mondiale, le Service corporatif de PD assure la surveillance et le contrôle, y compris la supervision de la conformité du Groupe Santander en matière de protection des données.

1.4 D'autre part, le Programme d'audit consiste en l'évaluation formelle et indépendante effectuée par la troisième ligne de défense (3LoD) afin d'assurer la conformité à la Politique, comme l'exigent les autorités de contrôle compétentes. L'avis fourni par Audit (3LoD) est un avis indépendant et ne se substitue pas aux responsabilités de contrôle et de surveillance incombant à la 1LoD et à la 2LoD, lesquelles feront également partie du périmètre d'audit lors de l'examen de l'intégration et de la mise en œuvre de la présente Politique.

2. APPROCHE

2.1 Vue d'ensemble de l'audit

L'entité responsable de réaliser les audits de conformité à la Politique et de s'assurer que ces audits couvrent tous les aspects de la Politique peut varier en fonction des circonstances spécifiques à chaque Membre du Groupe. En règle générale, les audits sont supervisés par des auditeurs internes ou externes accrédités, le cas échéant (qui bénéficient d'une indépendance garantie dans l'exercice de leurs fonctions relatives à ces audits). L'auditeur concerné sera responsable de veiller à ce que tout problème ou cas de non-conformité soit porté à l'attention de la haute direction et que les actions correctives visant à assurer la conformité soient mises en œuvre dans des délais raisonnables.

2.2 Calendrier et étendue de l'audit

2.2.1 Le département d'Audit interne, conformément à sa méthodologie d'évaluation des risques, déterminera le calendrier des audits dans le cadre d'un cycle d'audit d'une durée maximale de quatre ans.

Toutefois, les premiers audits auront lieu dans les 24 premiers mois suivant l'approbation formelle de la Politique, qui la rendra alors applicable. Par la suite, l'audit sera effectué conformément à la méthodologie d'audit fondée sur les risques applicable, comme indiqué au premier paragraphe de la présente section 2.2.

Dans tous les cas, les Membres du Groupe seront tenus d'effectuer un audit lorsque (i) il existe des indices de non-conformité à la présente Politique ; ou (ii) un audit spécifique (*ad hoc*) est demandé par l'Équipe de protection de la vie privée.

2.2.2 Dans le même ordre d'idées, le périmètre et l'étendue de l'audit seront déterminés par le département d'Audit interne, conformément à une analyse fondée sur les risques, réalisée selon la méthodologie approuvée.

2.2.3 Tous les aspects de la présente Politique (par exemple, applications, systèmes informatiques, transferts ultérieurs, etc.), y compris les méthodes et les plans d'action garantissant que les actions correctives ont été mises en œuvre, feront l'objet d'examens menés selon une approche fondée sur les risques afin de déterminer le périmètre spécifique de l'audit ; ces examens auront lieu, comme décrit ci-dessus, à des intervalles réguliers appropriés.

2.3 Auditeurs

2.3.1 Les audits au titre des présentes seront effectués par des auditeurs internes du département d'Audit interne ou des auditeurs externes accrédités, le cas échéant. Lorsque des audits sont réalisés par des auditeurs externes, les conditions suivantes doivent être respectées :

(a) Procéder à une diligence raisonnable appropriée avant sa sélection afin de s'assurer que les auditeurs concernés disposent des qualifications et du statut appropriés pour contribuer à cet exercice ; et

(b) Conclure un contrat avec les auditeurs afin de régir la fourniture de ses services conformément à la réglementation applicable.

2.4 Indépendance

2.4.1 Les personnes chargées de décider du programme d'audit ou de réaliser les audits bénéficient d'une indépendance garantie dans l'exercice de leurs fonctions.

2.5 Rapport

2.5.1 À l'issue de l'audit, selon sa nature, le rapport et les conclusions seront mis à la disposition de la haute direction, du Service corporatif de PD, du DPD ou du Champion concerné, et ils seront communiqués au Comité d'audit du Conseil d'administration ainsi qu'au Conseil d'administration du Membre soumis aux REC responsable. Le rapport d'audit comportera également des détails concernant toute action corrective requise, des recommandations, ainsi que les délais de mise en œuvre des actions correctives.

2.5.2 Les Membres du Groupe ont convenu de fournir, sur demande de toute autorité de contrôle compétente, des copies des résultats de tout audit de la Politique.

2.5.3 Le DPD ou le Champion concerné sera chargé d'assurer la liaison avec les autorités de contrôle compétentes afin de fournir les informations décrites ci-dessus.

ANNEXE 2

PROCEDURE DE TRAITEMENT DES RECLAMATIONS

1. INTRODUCTION

1.1 La présente Procédure de traitement des réclamations a pour objet d'expliquer comment seront traitées les réclamations introduites par une personne concernée dont les données à caractère personnel sont traitées par les Membres du Groupe conformément à la Politique.

2. COMMENT LES PERSONNES CONCERNEES PEUVENT DEPOSER UNE RECLAMATION

Toutes les réclamations des personnes concernées dont les données à caractère personnel sont traitées conformément à la présente Politique peuvent être adressées par écrit (y compris par e-mail) au DPD ou au Champion concerné, le cas échéant. Les personnes concernées peuvent déposer une réclamation en utilisant les coordonnées suivantes :

À l'attention : Équipe de protection de la vie privée

Adresse : [indiquer l'adresse postale]

E-mail : La liste des adresses e-mail pertinentes est disponible ici.

En tout état de cause, si des réclamations sont déposées par tout autre moyen, elles seront également traitées, à condition qu'elles soient dûment notifiées au Membre du Groupe concerné.

3. QUI TRAITE LES RECLAMATIONS ?

3.1 Le DPD ou le Champion concerné, selon le cas, traitera toutes les réclamations formulées au titre de la Politique relatives au traitement des données à caractère personnel. Le DPD ou le Champion, le cas échéant, se mettra en relation avec les unités opérationnelles concernées pour enquêter sur la réclamation et coordonnera une réponse (qui devra inclure des informations sur les mesures prises et communiquées à l'auteur de la réclamation).

3.2 Quel est le délai de réponse ?

Le DPD ou le Champion, avec le soutien de l'Équipe de protection de la vie privée, enverra à la personne concernée un accusé de réception de sa réclamation dans les dix jours ouvrables, mènera l'enquête et apportera ensuite une réponse de fond en fournissant des informations sur les mesures prises, sans retard injustifié et en tout état de cause dans un délai d'un mois civil. Si, en raison de la complexité de la réclamation ou du nombre de demandes, une réponse de fond ne peut pas être fournie dans ce délai, le DPD ou le Champion, avec le soutien de l'Équipe de protection de la vie privée, informera l'auteur de la réclamation des raisons du retard dans un délai d'un mois civil à compter de la réception de la réclamation et fournira une estimation raisonnable du délai (n'excédant pas deux mois civils supplémentaires à compter de la date à laquelle la personne concernée a été informée de la prolongation) pour la réponse.

Si le délai de réponse n'est pas respecté et que la réponse à la réclamation est retardée sans motif dûment communiqué, la personne concernée peut en informer le DPD ou le Champion, qui, sans retard injustifié et en tout état de cause dans un délai de dix jours calendaires, expliquera les raisons d'un tel retard et informera la personne concernée des mesures prises jusqu'à présent. L'affaire sera

transmise au Service corporatif de PD (accompagnée d'un rapport motivé déterminant les mesures à prendre), et celui-ci examinera le dossier et conseillera le DPD ou le Champion sur la manière de résoudre les problèmes faisant l'objet de la réclamation dans les plus brefs délais. En tout état de cause, la personne concernée peut également exercer les droits décrits à la section 3.4 de la présente Annexe 2.

3.3 Lorsque l'auteur d'une réclamation conteste une conclusion ou le rejet d'une réclamation

Si une réclamation est jugée fondée, le DPD ou le Champion prendra les mesures nécessaires pour résoudre le problème soulevé par la personne concernée et l'informera en conséquence.

Si l'auteur de la réclamation conteste la réponse du DPD ou du Champion (y compris si cette réponse consiste en un refus de traiter/de donner suite à la réclamation) ou tout aspect d'une conclusion, il ou elle peut en informer le DPD ou le Champion concerné en conséquence. L'affaire sera transmise au Service corporatif de PD qui examinera le dossier et, par l'intermédiaire du DPD ou du Champion de l'entité, informera l'auteur de la réclamation de la décision finale d'accepter la conclusion initiale ou de la remplacer par une nouvelle conclusion. Le Service de PD local concerné répondra à l'auteur de la réclamation dans un délai d'un mois civil à compter de sa saisine. Si, en raison de la complexité de la réclamation, il n'est pas possible de fournir une réponse de fond dans ce délai, le Service corporatif de PD informera l'auteur de la réclamation du motif du retard dans le mois civil suivant la réception de la saisine et fournira une estimation raisonnable du délai de réponse (ne dépassant pas deux mois civils supplémentaires). Si la réclamation est jugée fondée, le Service corporatif de PD veillera à ce que toutes les mesures nécessaires soient prises en conséquence.

3.4 Mécanismes de réclamation alternatifs

Les personnes concernées dont les données à caractère personnel sont traitées conformément à la présente Politique ont également le droit de : (i) déposer une réclamation auprès de l'autorité de contrôle de l'État membre dans lequel la violation alléguée a eu lieu, ou dans lequel la personne concernée travaille ou réside habituellement ; et/ou (ii) introduire un recours devant une juridiction compétente dans le pays européen où le Membre du Groupe est établi ou dans le pays européen où la personne concernée réside. Comme précisé plus en détail aux Sections C.2 à C.4, lorsqu'un manquement est commis par un Membre du Groupe situé en dehors de l'EEE, les personnes concernées conservent le droit de déposer des réclamations auprès du Membre soumis aux REC responsable désigné et d'intenter des actions à son encontre, comme si le manquement avait été commis par cette entité dans l'État membre où elle est établie. Ces droits s'appliqueront, qu'ils aient ou non préalablement déposé une réclamation auprès d'un Membre du Groupe dans le cadre de la présente Procédure de traitement des réclamations.

ANNEXE 3

PROCEDURE DE COOPERATION

1. PROCEDURE DE COOPERATION

1.1 Cette Procédure de coopération définit la manière dont les Membres du Groupe coopéreront avec et accepteront d'être audités et inspectés par les autorités de contrôle compétentes (y compris, si nécessaire, sur site) dans le cadre de la présente Politique ; ainsi que de prendre en compte leurs avis et de se conformer à leurs décisions sur toute question relative à la présente Politique.

1.2 Le cas échéant, Les Membres du Groupe mettront à disposition le personnel approprié pour dialoguer avec l'autorité de contrôle compétente au sujet de la Politique.

1.3 Sur demande, le DPD ou le Champion concerné ou le département d'Audit interne, selon le cas, fournira, à toute autorité de contrôle compétente, des copies des résultats de tout audit de la Politique effectué conformément à l'Annexe 1, ainsi que toute information relative aux opérations de traitement couvertes par la Politique, à laquelle il sera rappelé, lors de la réception de ces informations, son devoir de secret professionnel.

1.4 Les Membres du Groupe conviennent que les autorités de contrôle compétentes peuvent procéder à un audit en matière de protection des données ou une inspection (y compris, si nécessaire, sur site) à leur égard conformément à la Législation européenne en matière de protection de données applicable à l'Entité exportatrice concernée.

1.5 Tous les Membres du Groupe acceptent d'être audités par les autorités de contrôle compétentes, conformément aux procédures d'audit applicables de ces autorités de contrôle.

1.6 Les Membres du Groupe conviennent que tout litige relatif à l'exercice, par une autorité de contrôle compétente, de ses pouvoirs de contrôle au titre de la présente Politique sera tranché par les tribunaux de l'État membre où est située ladite autorité de contrôle, conformément au droit procédural dudit État membre.

ANNEXE 4

PROCEDURE DE MISE A JOUR

1. INTRODUCTION ET PRINCIPES GENERAUX

1.1 La présente Procédure de mise à jour définit la manière dont les modifications apportées à la Politique seront communiquées aux autorités de contrôle compétentes, aux personnes concernées et aux Membres du Groupe soumis à la Politique.

1.2 La Politique sera tenue à jour afin de refléter la situation et le contexte actuels en matière de protection des données personnelles.

2. MODIFICATIONS IMPORTANTES APPORTEES A LA POLITIQUE

2.1 Le DPD de Banco Santander et Corporate Legal communiqueront à l'avance toute modification substantielle de la Politique (c'est-à-dire, toute modification susceptible d'être préjudiciable au niveau de protection offert par la Politique ou d'affecter de manière significative la Politique –par exemple, des changements concernant son caractère contraignant–) à l'Agence espagnole de protection des données (l'« **Autorité responsable des REC** ») et, via l'Autorité responsable des REC, aux autorités de contrôle. Cette communication doit comporter une brève explication des motifs de la mise à jour. L'autorité de contrôle compétente évaluera également si les modifications apportées nécessitent une nouvelle approbation.

3. AUTRES MODIFICATIONS DE LA POLITIQUE

3.1 Le DPD de Banco Santander et Corporate Legal communiqueront à l'Autorité responsable des REC (et, par l'intermédiaire de celle-ci aux autres autorités de contrôle concernées), sur demande et au moins une fois par an, les modifications apportées à la Politique (ou l'absence de celles-ci). La mise à jour annuelle comprendra également le renouvellement de la confirmation selon laquelle le Membre soumis aux REC responsable dispose d'actifs suffisants, ou a pris des dispositions appropriées lui permettant de verser une indemnisation pour les dommages résultant d'une violation de la Politique.

3.2 À titre d'exemple, les modifications susmentionnées peuvent inclure celles de nature administrative (y compris les mises à jour de la liste des Membres du Groupe) ; celles intervenues à la suite d'une modification de la Législation européenne en matière de protection de données applicable ; ou celles résultant de toute mesure législative, de toute décision de justice, ou de toute mesure ou ligne directrice émanant d'une autorité de contrôle (y compris les lignes directrices du Comité européen de la protection des données). Banco Santander fournira également une brève explication à l'Autorité responsable des REC et aux autres autorités de contrôle des raisons de toute modification notifiée de la Politique.

4. NOUVEAUX MEMBRES DU GROUPE

4.1 Les DPD et les Champions (avec l'Équipe de protection de la vie privée) veilleront à ce que tous les nouveaux Membres du Groupe soient effectivement soumis à la Politique et puissent s'y conformer, avant d'effectuer un transfert de données à caractère personnel vers des Membres du Groupe.

5. COMMUNICATION ET CONSIGNATION DES MODIFICATIONS APPORTEES A LA POLITIQUE

5.1 La Politique contient un historique des modifications qui précise les dates des révisions de la Politique ainsi que les détails des révisions effectuées. Corporate Legal tiendra à jour la liste des modifications apportées à la Politique et le Service corporatif de PD tiendra à jour la liste des Membres du Groupe soumis à ladite Politique.

5.2 Corporate Legal, avec le soutien du Service corporatif de PD, communiquera toutes les modifications apportées à la Politique, qu'elles soient significatives ou non :

(a) aux Membres du Groupe assujettis à la Politique, sans retard injustifié, et publiera une version mise à jour de cette Politique sur le réseau interne du Groupe Santander ;

(b) de manière systématique aux personnes concernées qui bénéficient de la Politique, via le site web de la société (Web Corporativa Santander) ; et

(c) sur demande et, par l'intermédiaire des DPD locaux concernés (ou d'une fonction similaire), à l'autorité de contrôle compétente.