GRUPO SANTANDER

POLÍTICA DE REGRAS VINCULATIVAS APLICÁVEIS ÀS EMPRESAS – RESPONSÁVEL PELO TRATAMENTO

ÍNDICE PÁGINA

INTRODUÇÃO

A presente Política de regras vinculativas aplicáveis às empresas – Responsável pelo tratamento e os respetivos Anexos (em conjunto, a «**Política**») estabelecem a abordagem adotada pelo Banco Santander, S.A. («**Banco Santander**») no que respeita à proteção e gestão de dados pessoais pelos Membros do Grupo Santander, conforme definido abaixo, que aderiram à Política no contexto de transferências internacionais dos referidos dados pessoais entre Membros do Grupo, conforme definido abaixo.

O Banco Santander é a sociedade-mãe e a sede de um dos maiores grupos financeiros de Espanha, composto por filiais espanholas e estrangeiras («**Grupo Santander**»), dedicado à prestação de serviços financeiros a nível mundial, principalmente nas seguintes áreas: (i) **Banca Comercial e de Retalho**: que abrange todas as operações de banca comerciais e de retalho do Santander; (ii) **Banca de Empresas e Investimento**: que presta apoio a clientes empresariais e institucionais através de serviços personalizados e produtos grossistas de valor acrescentado, por intermédio das divisões Mercados, Banca de Investimento (Financiamento Global da Dívida e Financiamento das Empresas) e Banca Transacional Global; (iii) **Gestão de Património e Seguros**: que reúne as atividades de banca privada, gestão de ativos e seguros através do Santander Private Banking, Santander Asset Management e Santander Insurance; (iv) **Banco Digital do Consumidor**: que reúne a plataforma digital Openbank e o Santander Consumer Finance, criando um modelo único em todos os mercados para os consumidores e a atividade de financiamento automóvel; e (v) **PagoNxt e Cartões**: que abrange a PagoNxt, onde se concentram todas as atividades de pagamento do Santander, e a Global Cards, que representa a atividade e plataforma de cartões do Santander, disponibilizando opções de pagamento digital e soluções de tecnologia global aos bancos do Santander e a novos clientes. Além do acima exposto, o Grupo Santander integra igualmente o **Centro Corporativo e outras funções ao serviço do Grupo**: que correspondem às áreas responsáveis pela prestação de apoio e assistência aos Membros do Grupo na execução das ações necessárias para o grupo que não estejam estritamente relacionadas com a respetiva atividade principal (por exemplo, gestão de colaboradores, cumprimento de obrigações legais, auditorias, gestão do risco, etc.).

Além de outras definições previstas na presente Política, aplicam-se os seguintes termos:

«**Legislação Local Aplicável em matéria de Proteção de Dados**», qualquer legislação nacional ou local em matéria de proteção de dados (incluindo, consoante o caso, a Legislação Europeia em matéria de Proteção de Dados) aplicável aos Membros do Grupo, desde que a mesma respeite a essência dos direitos e liberdades fundamentais e não exceda o que é considerado necessário e proporcional numa sociedade democrática, em conformidade com os requisitos previstos na Regra 13 da presente Política;

«**autoridade de controlo competente**», a autoridade de controlo do EEE competente para lidar com a Entidade Exportadora;

«**responsável pelo tratamento**», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais;

«**Europa**» ou «**EEE**», os países que integram o Espaço Económico Europeu;

«**Legislação Europeia em matéria de Proteção de Dados**», o RGPD e qualquer legislação de proteção de dados de um Estado-Membro europeu, incluindo a legislação nacional que dá execução aos requisitos do RGPD, como a legislação subordinada, conforme alterada periodicamente;

«**Entidade Exportadora**», um Membro do Grupo estabelecido na Europa, ou de outro modo sujeito à Legislação Europeia em matéria de Proteção de Dados, que transfere, ou de outro modo disponibiliza, dados pessoais a uma Entidade Importadora ao abrigo da presente Política;

«**RGPD**», o Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados);

«**Membro do Grupo**», os membros do Grupo Santander que aderiram à presente Política;

«**Entidade Importadora**», um Membro do Grupo estabelecido fora da Europa que recebe dados pessoais de uma Entidade Exportadora e procede ao tratamento dos dados pessoais transferidos fora do EEE;

«**Membro Responsável pelas RVE**», o Banco Santander (ou seja, o Banco Santander, S.A., conforme definido acima);

«**dados pessoais**», informação relativa a uma pessoa singular identificada ou identificável. É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

«**tratamento**», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

«**subcontratante**», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

«**definição de perfis**», qualquer forma de tratamento automatizado de dados pessoais que consista na avaliação dos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais ou interesses, fiabilidade ou comportamento, localização ou deslocações;

«**categorias especiais de dados pessoais**» ou «**dados sensíveis**», os dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como os dados genéticos, os dados biométricos tratados com o objetivo de identificar uma pessoa singular de forma inequívoca, os dados relativos à saúde ou os dados relativos à vida sexual ou à orientação sexual de uma pessoa singular; e

«**autoridade de controlo**», uma autoridade pública independente criada por um Estado-Membro numa jurisdição europeia, o qual é responsável por fiscalizar a aplicação da Legislação Europeia em matéria de Proteção de Dados, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados no EEE.

A presente Política aplica-se a todos os dados pessoais sujeitos à Legislação Europeia em matéria de Proteção de Dados que sejam posteriormente transferidos das Entidades Exportadoras para as Entidades Importadoras, bem como às transferências ulteriores efetuadas pelas Entidades Importadoras para outras Entidades Importadoras ou para terceiros fora do EEE (em conformidade com os requisitos previstos na Regra 6 abaixo). Por conseguinte, todas as obrigações e os requisitos atribuídos aos Membros do Grupo ao abrigo da presente

Política serão aplicáveis na medida em que digam respeito a dados pessoais abrangidos pelo respetivo âmbito de aplicação.

A presente Política aplica-se aos referidos dados pessoais tratados pelos Membros do Grupo, conforme descrito nas secções «*Que dados pessoais são abrangidos pela presente Política?*» e «*Para que finalidades são transferidos os dados pessoais ao abrigo da presente Política?*».

Os Membros do Grupo e os respetivos colaboradores devem cumprir e respeitar, na íntegra, a presente Política no âmbito do tratamento de dados pessoais aqui descritos.

Esta Política é complementar e não substitui nem prevalece sobre quaisquer requisitos ou regras específicos relativos à confidencialidade ou ao dever de sigilo que possam aplicar-se a uma área ou função de negócio do Grupo Santander ou que sejam exigidos pela legislação aplicável (desde que a referida legislação cumpra os requisitos previstos na Regra 13 da presente Política).

A presente Política, juntamente com a lista atual dos Membros do Grupo e os respetivos dados de contacto, conforme incluídos no Anexo 5, é publicada no sítio Web da empresa, acessível ao público aqui.

Aplicação às transferências efetuadas por Membros do Grupo não sujeitas à Legislação Europeia em matéria de Proteção de Dados

Se um Membro do Grupo que não esteja sujeito à Legislação Europeia em matéria de Proteção de Dados também tiver restrições relativas às transferências internacionais de dados pessoais ao abrigo da respetiva Legislação Local Aplicável em matéria de Proteção de Dados e as autoridades locais desse país reconhecerem a presente Política (no todo ou em parte, conforme exigido pela Legislação Local Aplicável em matéria de Proteção de Dados) como um mecanismo válido para legitimar as transferências internacionais de dados pessoais, a presente Política poderá também aplicar-se aos dados pessoais transferidos desses países para as Entidades Importadoras. Para efeitos de clarificação, o disposto na presente Política não prejudica a aplicação da Legislação Local Aplicável em matéria de Proteção de Dados ao Membro do Grupo estabelecido fora da Europa.

Nestes casos, as definições acima devem ser interpretadas no sentido de considerar como Entidade Exportadora o Membro do Grupo que transfere os dados pessoais que não estão sujeitos à Legislação Europeia em matéria de Proteção de Dados. Assim, a presente Política deve ser interpretada e aplicada *mutatis mutandis* (por exemplo, a Legislação Europeia em matéria de Proteção de Dados deve ser entendida como a Legislação Local Aplicável em matéria de Proteção de Dados, a autoridade de controlo competente como a autoridade local competente na jurisdição pertinente ou o Estado-Membro como o país em causa).

Neste contexto, o Membro do Grupo que transfere os dados pessoais que não estão sujeitos à Legislação Europeia em matéria de Proteção de Dados atuará como o Membro Responsável pelas RVE relativamente às referidas transferências internacionais de dados.

PARTE I: CONTEXTO E MEDIDAS

O QUE É A LEGISLAÇÃO EUROPEIA EM MATÉRIA DE PROTEÇÃO DE DADOS?

A Legislação Europeia em matéria de Proteção de Dados confere às pessoas o direito de controlar a forma como os seus dados pessoais são tratados. Ao abrigo da Legislação Europeia em matéria de Proteção de Dados, quando uma organização trata dados pessoais para as suas próprias finalidades, considera-se que a mesma é responsável pelo tratamento das referidas informações, sendo, por conseguinte, a principal responsável pelo cumprimento dos requisitos legais. Por exemplo, quando atuamos na qualidade de entidade empregadora, somos responsáveis pelo tratamento dos dados pessoais que tratamos relativamente aos nossos colaboradores.

Por outro lado, quando uma organização trata informações por conta de outra entidade (por exemplo, para prestar um serviço), considera-se que a primeira atua na qualidade de subcontratante dos dados.

DE QUE FORMA É QUE A LEGISLAÇÃO EUROPEIA EM MATÉRIA DE PROTEÇÃO DE DADOS AFETA AS TRANSFERÊNCIAS DE DADOS PESSOAIS ENTRE MEMBROS DO GRUPO?

A Legislação Europeia em matéria de Proteção de Dados não permite a transferência de dados pessoais para países, territórios ou organizações internacionais situados fora da Europa que não assegurem um nível de proteção adequado dos direitos das pessoas em matéria de proteção de dados. Uma vez que alguns dos países onde os Membros do Grupo operam não são considerados pela Comissão Europeia como assegurando um nível de proteção adequado, é necessário estabelecer garantias apropriadas que permitam cumprir os requisitos da Legislação Europeia em matéria de Proteção de Dados.

O QUE ESTÃO OS MEMBROS DO GRUPO A FAZER A ESSE RESPEITO?

Os Membros do Grupo devem adotar as medidas adequadas para assegurar que o tratamento de dados pessoais, quando estes são transferidos a nível internacional, é efetuado de forma segura e legal. Assim, a presente Política tem por objetivo estabelecer um quadro que cumpra os requisitos da Legislação Europeia em matéria de Proteção de Dados e, consequentemente, assegure um nível de proteção adequado para todos os dados pessoais que são transferidos das Entidades Exportadoras para as Entidades Importadoras.

A presente Política é juridicamente vinculativa e aplica-se a todos os Membros do Grupo e aos respetivos colaboradores sempre que os Membros do Grupo tratem dados pessoais, quer por meios manuais, quer por meios automatizados. Exige que os Membros do Grupo cumpram as Regras definidas na Parte II (consoante aplicável), juntamente com as políticas e os procedimentos previstos nos Anexos da Parte III da presente Política. Se uma Entidade Importadora estiver sujeita a uma Legislação Local Aplicável em matéria de Proteção de Dados que seja reconhecida como assegurando um nível de proteção adequado ao abrigo da Legislação Local Aplicável em matéria de Proteção de Dados da Entidade Exportadora e proporcionar um nível de proteção equivalente ao nível previsto nesta Política, os processos e procedimentos locais que cumpram, em termos substanciais, os requisitos da presente Política serão considerados válidos, ainda que introduzam variações ou diferenças de natureza processual (por exemplo, a intervenção de equipas locais na execução de determinados procedimentos), desde que as referidas variações sejam compatíveis com a presente Política. As transferências internacionais abrangidas pela presente Política incluem as transferências de dados pessoais de Membros do Grupo abrangidas pelo âmbito de aplicação territorial do RGPD, nos termos do artigo 3.º do RGPD, para Membros do Grupo situados fora do EEE, bem como as transferências ulteriores para outros Membros do Grupo ou para terceiros externos (em conformidade com os requisitos previstos na Regra 6 abaixo) situados fora do EEE.

O QUE ACONTECE AOS MEMBROS DO GRUPO QUE EXPORTAM DADOS E NÃO ESTÃO SUJEITOS À LEGISLAÇÃO EUROPEIA EM MATÉRIA DE PROTEÇÃO DE DADOS?

Conforme explicado na Introdução e com o objetivo de definir um quadro global de proteção de dados para o Grupo Santander, se um Membro do Grupo que não esteja sujeito à Legislação Europeia em matéria de Proteção de Dados também tiver restrições relativas às transferências internacionais de dados pessoais ao abrigo da respetiva Legislação Local Aplicável em matéria de Proteção de Dados e as autoridades locais desse país reconhecerem a presente Política (no todo ou em parte, conforme exigido pela Legislação Local Aplicável em matéria de Proteção de Dados) como um mecanismo válido para legitimar as transferências internacionais de dados pessoais, a presente Política poderá também aplicar-se aos dados pessoais transferidos desses países para as Entidades Importadoras. Para efeitos de clarificação, o disposto na presente Política não prejudica a aplicação da Legislação Local Aplicável em matéria de Proteção de Dados ao Membro do Grupo estabelecido fora da Europa.

QUE DADOS PESSOAIS SÃO ABRANGIDOS PELA PRESENTE POLÍTICA?

Os dados pessoais tratados ao abrigo da presente Política incluem:

- Dados pessoais de **colaboradores atuais e antigos, bem como de outros membros do pessoal (tais como estagiários, trabalhadores destacados e contratantes independentes)**:

  (a) Dados pessoais e de contacto (por exemplo, nome próprio, nome do meio, apelido, designação, pseudónimo, assinatura, género, data de nascimento, nacionalidade, números/documentos de identificação nacional, endereço de e-mail, morada, números de telefone, fotografia, autorizações de trabalho, etc.); **(b) Dados de emprego, incluindo o percurso profissional, as condições de trabalho e os dados de contacto** (por exemplo, endereço de e-mail e número de telefone profissionais, número de identificação do colaborador, atribuição de chaves de nome de utilizador/endereço (isto é, chaves utilizadas para aceder ao terminal do posto de trabalho), percurso profissional, cargo atual, função, tarefas, empresa, centro de negócios, unidade de negócios, número de identificação do departamento, número de identificação da sucursal, país de atividade, ID e nome do(s) supervisor(es), ID e nome do(s) subordinado(s), situação e tipo de vínculo laboral, indicação de o colaborador ser ou não externo, data de admissão, data de início de funções, data de cessação (quando aplicável), dados contratuais, planos de reforma, modalidades de flexibilidade laboral, pedidos de mobilidade, dotação, dados relativos ao cumprimento das políticas internas ou outras políticas legais aplicáveis, avaliações e classificações de desempenho (incluindo comentários de gestores, partes interessadas e outras pessoas que trabalhem com o colaborador), promoções e registos disciplinares, etc.); **(c) Dados relativos ao talento, ao recrutamento e às candidaturas, bem como às habilitações académicas e à formação** (por exemplo, informações constantes de cartas de candidatura e do currículo, informações relativas ao plano de desenvolvimento e à respetiva avaliação, dados de formação, sítio Web pessoal ou perfil no LinkedIn fornecidos diretamente pelos colaboradores, experiência profissional anterior e referências, percurso académico, qualificações profissionais, competências linguísticas e outras competências relevantes, etc.); **(d) Informações financeiras, incluindo dados relativos ao processamento salarial e à remuneração** (por exemplo, dados da conta bancária, salário, planos de benefícios, prémios, moeda, retribuição variável, informações sobre opções de compra de ações, atribuição de ações e outros tipos de prémio, periodicidade dos pagamentos, data de entrada em vigor da remuneração atual, revisões salariais, número de identificação fiscal e código fiscal, etc.); **(e) Dados de segurança e TI** (por exemplo, ID de utilizador, chaves de acesso a ferramentas, dados de início de sessão, credenciais e perfis de segurança, mensagens de e-mail enviadas e recebidas através das contas de e-mail da empresa (na medida dos limites legalmente permitidos), informações recolhidas através da utilização dos sistemas de TI, incluindo dados de acesso e autenticação, histórico de navegação na Internet, números de telefone marcados, documentos e ficheiros armazenados nos sistemas ou redes da empresa (incluindo os ambientes de trabalho dos computadores), registos de atividade, endereço IP, tentativas de início de

sessão bem-sucedidas e falhadas, informações recolhidas através de cookies ou outras tecnologias de rastreio semelhantes, etc.); **(f) Dados relativos a horários de trabalho** (por exemplo, férias, dias e períodos de ausência, outras licenças e comprovativos dos respetivos motivos (quando aplicável), datas de regresso ao trabalho após licenças, outros dados relativos a ausências, registo das horas trabalhadas (quando legalmente exigido ou permitido), horas extraordinárias, turnos de trabalho, etc.); e **(g) Quaisquer outras informações fornecidas voluntariamente pelos titulares dos dados** (por exemplo, através de inquéritos de envolvimento ou outros inquéritos, etc.).

Além disso, as **categorias especiais de dados pessoais (nomeadamente, mas não exclusivamente, os dados relativos à saúde e à filiação sindical)** podem ser tratadas pelos Membros do Grupo quando tal seja necessário e exigido ou permitido pela legislação aplicável para as finalidades descritas na secção seguinte.

- Relativamente aos dados pessoais dos **familiares dos colaboradores**:

  (a) Dados pessoais e de contacto (por exemplo, nome próprio, apelido, género, números/documentos de identificação nacional, dados de contacto, como o número de telefone para contacto em caso de emergência, etc.); e **(b) Outras informações dos colaboradores relacionadas com os respetivos familiares ou relativas aos mesmos, quando legalmente exigidas ou permitidas** (por exemplo, agregado familiar e a respetiva situação, relação com o colaborador, nome e outras informações relevantes sobre filhos e outros dependentes, estado civil, dados relativos ao cumprimento das políticas internas ou outras políticas legais aplicáveis, etc.).

- Relativamente aos dados pessoais de **candidatos atuais e antigos**:

  (a) Dados pessoais e de contacto (por exemplo, nome próprio, apelido, país, estado e cidade de residência, endereço de e-mail, morada, números de telefone, nacionalidade, etc.); **(b) Dados relativos ao recrutamento, às habilitações académicas e à formação** (por exemplo, informações constantes de cartas de candidatura e do currículo, sítio Web pessoal ou perfil no LinkedIn fornecidos diretamente pelos candidatos, experiência profissional anterior e referências, percurso académico, qualificações profissionais, competências linguísticas e outras competências relevantes, informações sobre avaliações de desempenho, plano de desenvolvimento e disponibilidade para efeitos de mobilidade geográfica, dados pessoais resultantes da participação dos candidatos no processo de recrutamento, como, por exemplo, os dados obtidos durante a realização de entrevistas pessoais, as mensagens de e-mail trocadas no âmbito das candidaturas ou as conversas realizadas, etc.); e **(c) Informações áudio e visuais** (por exemplo, voz e imagem, tal como captadas em fotografias ou gravações de vídeo ou áudio, no contexto de entrevistas realizadas por telefone ou videoconferência, etc.).

- Relativamente aos dados pessoais de **potenciais clientes, consumidores e clientes** (incluindo dos respetivos colaboradores, representantes e/ou agentes, consoante aplicável, bem como dos utilizadores autorizados e utilizadores do sítio Web):

  (a) Dados pessoais e de contacto (por exemplo, nome próprio, segundo nome, apelido, número de telefone, endereço de e-mail, endereço postal, país de residência, região, cidadania ou nacionalidade, números/documentos de identificação nacional, género, idioma, data de nascimento, país de nascimento, estado civil, dados relativos à situação familiar ou social, como o número de dependentes, indicação de a pessoa ser ou não menor de idade ou necessitar de um representante legal, dados demográficos e socioeconómicos, etc.); **(b) Dados profissionais** (por exemplo, profissão, cargo, percurso profissional e académico, dados da empresa, dados de contacto profissionais, ocupação, categoria profissional, designação da função, etc.); **(c) Dados (pré-)contratuais** (por exemplo, código de categoria, capacidade jurídica, dados relacionados com procurações, número de registo e indicador interno de cliente, nível de vinculação, relação comercial com o Santander, produtos ou serviços

contratados ou solicitados, classificação de risco, informações de agências de crédito, ordens de compra, dados estatísticos, faturas, informações sobre bens e ativos, subvenções, informações sobre contas e operações, na medida permitida pela legislação aplicável, contratos e outros acordos que possam conter dados pessoais relativos a estes titulares dos dados e ao respetivo desempenho, etc.); **(d) Informações financeiras, fiscais e de pagamento** (por exemplo, dados de contas bancárias, dados dos beneficiários, saldos atuais e históricos de produtos e serviços e histórico de pagamentos, dados de cartões de crédito, pagamento direto de salários, dados/tipo de rendimentos, fundos disponíveis, operações monetárias, montante dos pagamentos, dados das remessas, dados de solvência, número de identificação fiscal, país de residência fiscal, saldo fiscal anual, etc.); **(e) Dados de conformidade** como o ID de PEP associado, DMIF ou relação semelhante (por exemplo, associados, vínculos familiares, etc.), o tipo de relação (por exemplo, cônjuge, familiar, acionista, representante legal, etc.), a data de início e, se aplicável, a data de fim da relação, informações relacionadas com as obrigações de CBC e prevenção de fraudes (perfis, informações e classificações de bases de dados de solvência e bases de dados de risco, etc.); **(f) Informações áudio e visuais** (por exemplo, voz e imagem captadas em fotografias, vídeos ou áudios, no contexto de reuniões realizadas por telefone ou videoconferência ou para fins de segurança, etc.); **(g) Informações de TI** (por exemplo, endereço IP, ID de utilizador, palavras-passe, registos, incluindo dados do perfil, dos sítios Web ou portais do Grupo Santander, chave de acesso a ferramentas, credenciais e perfis de segurança, dados de autenticação de TI, histórico de navegação, ID do dispositivo, ID de publicidade, redes sociais, etc.); e **(h) Outros dados relativos à relação profissional com o Grupo Santander** (por exemplo, dados de reclamações, comunicações partilhadas, preferências de comunicação, pedidos, etc.).

Além disso, as **categorias especiais de dados pessoais (incluindo dados pessoais relativos a condenações e infrações penais, no contexto de riscos e sanções internacionais)** podem ser tratadas pelos Membros do Grupo, quando tal seja necessário e exigido ou permitido pela legislação aplicável, para as finalidades descritas na secção seguinte.

- Relativamente aos dados pessoais de **potenciais e atuais fornecedores, vendedores ou prestadores de serviços** (incluindo dos respetivos colaboradores, representantes e/ou agentes, consoante aplicável):

  (a) Dados pessoais, profissionais e de contacto (por exemplo, nome próprio, apelido, número de telefone, endereço de e-mail, endereço postal, números/documentos de identificação nacional, cargo/função, dados da empresa, dados de contacto profissionais, etc.); **(b) Dados contratuais** (por exemplo, dados relacionados com procurações, ordens de compra, faturas, contratos e outros acordos que possam conter dados pessoais relativos a estes titulares dos dados, etc.); **(c) Informações financeiras e de pagamento** (por exemplo, dados de contas bancárias, dados de cartões de crédito, dados de solvência, etc.); **(d) Informações áudio e visuais** (por exemplo, voz e imagem captadas em fotografias, vídeos ou áudios, no contexto de reuniões realizadas por telefone ou videoconferência ou para fins de segurança (incluindo informações captadas através de sistemas de entrada e câmaras de segurança), etc.); **(e) Informações de TI** (por exemplo, endereço IP, ID de utilizador, palavras-passe, registos, incluindo dados do perfil, dos sítios Web ou portais do Grupo Santander, etc.); e **(f) Outros dados relativos à relação profissional com o Grupo Santander** (por exemplo, dados de reclamações, comunicações partilhadas, etc.).

- Relativamente aos dados pessoais dos **acionistas**:

  (a) Dados pessoais, profissionais e de contacto (por exemplo, nome próprio, apelido, género, data de nascimento, número de telefone, endereço de e-mail, endereço postal, números/documentos de identificação nacional, cargo/função, dados da empresa, dados de contacto profissionais, número de acionista, nacionalidade/cidadania, país de nascimento e residência, etc.); **(b) Informações financeiras e de pagamento** (por exemplo, dados de contas bancárias, dados de cartões de crédito, dados de

pagamento, quantidade de ações, documentação relativa a titularidade e dividendos, operações monetárias, movimentos, posições e participações em ações de outras sociedades, informações sobre produtos financeiros contratados, etc.); e **(c) Informações de TI** (por exemplo, endereço IP, ID de utilizador, palavras-passe, registos, incluindo dados do perfil, dos sítios Web ou portais do Grupo Santander, etc.).

- Relativamente aos dados pessoais dos **utilizadores da Web, utilizadores finais e utilizadores institucionais (incluindo os utilizadores de plataformas/sítios Web/aplicações relacionados com universidades, emprego e empreendedorismo):**

  (a) Dados pessoais e de contacto (por exemplo, nome próprio, apelido, data de nascimento, género, endereço de e-mail, endereço postal, números de telefone, país de residência, nacionalidade, números de identificação nacional, etc.); **(b) Dados profissionais e académicos** (por exemplo, cargo/função, dados da empresa, dados de contacto profissionais, percurso profissional, currículo, dados académicos, habilitações académicas ou qualificações, dados demográficos e socioeconómicos, ligação a projetos empresariais ou empresas, etc.); **(c) Informações de TI** (por exemplo, endereço IP, ID de utilizador, palavras-passe, registos relativos à utilização, incluindo dados do perfil, de sítios Web ou portais, registos de chamadas, etc.); **(d) Dados de navegação e utilização** (por exemplo, informações recolhidas automaticamente junto dos titulares dos dados (ou seja, através de cookies ou outras tecnologias semelhantes) relativas à utilização de sítios Web/dispositivos (incluindo perfis), navegação na Web, dados de utilização, etc.); e **(e) Outros dados relativos à relação com o Grupo Santander** (por exemplo, consultas, interesses, comunicações partilhadas, etc.).

PARA QUE FINALIDADES SÃO TRANSFERIDOS OS DADOS PESSOAIS AO ABRIGO DA PRESENTE POLÍTICA?

Os dados pessoais são transferidos entre os Membros do Grupo a nível mundial (principalmente Argentina, Baamas, Brasil, Colômbia, países da Europa, México, Peru, Suíça, Reino Unido, Estados Unidos da América, Uruguai, etc.) ao abrigo da presente Política, para as seguintes finalidades e apenas na medida dos limites permitidos pela legislação aplicável:

- As transferências de dados pessoais de **colaboradores atuais e antigos, bem como de outros membros do pessoal (tais como estagiários, trabalhadores destacados ou contratantes independentes)** são efetuadas para as seguintes finalidades: **(a) administrar e gerir o pessoal** (por exemplo, gestão da formação, planeamento e monitorização, gestão do desempenho, gestão de salários e benefícios, promoções, planeamento da sucessão e desenvolvimento de carreira, gestão da mobilidade interna, transferências e destacamentos, elaboração e gestão dos diretórios atuais de colaboradores, organização de viagens em serviço, gestão de despesas profissionais e dos respetivos reembolsos, facilitação de comunicações, negociações, operações e conferências no âmbito da atividade empresarial, verificação do cumprimento das obrigações e dos deveres laborais dos colaboradores, gestão de licenças, ausências e avaliações e reporte de processos disciplinares e cessações, revisão de decisões em matéria de emprego, avaliação e tomada de decisões relacionadas com a aptidão dos colaboradores para o trabalho e adaptações dos postos de trabalho, monitorização do cumprimento das políticas e dos procedimentos internos e de outras atividades de monitorização exigidas pela legislação aplicável (por exemplo, sistemas internos de denúncia), incluindo o cumprimento do Código de Conduta nos Mercados de Valores Mobiliários ou o cumprimento de políticas semelhantes e das respetivas obrigações, incluindo a aprovação e monitorização de operações de contas pessoais, a realização de análises e planeamento da força de trabalho, a realização de verificações de antecedentes, conforme exigidas ou permitidas pela legislação aplicável, etc.); **(b) realizar segmentações agregadas, estatísticas e análises** relativas aos dados da atividade dos colaboradores, a fim de melhorar o conhecimento da população de colaboradores e apoiar a tomada de decisões, nomeadamente em matéria de recrutamento de talento, planeamento de carreira e planeamento da sucessão; **(c) apoiar a gestão dos serviços prestados pelo Grupo Santander e das respetivas operações comerciais** (por exemplo, gestão e

proteção dos sistemas e infraestruturas de TI e comunicações, gestão e afetação de ativos da empresa e recursos humanos, equipamentos de escritório e outros bens, planeamento operacional e estratégico, gestão de projetos, continuidade do negócio, compilação de pistas de auditoria e outras ferramentas de reporte, manutenção de registos relativos às atividades empresariais, orçamentação, gestão e reporte financeiros, comunicações, gestão de fusões, aquisições, reorganizações ou alienações, etc.); e **(d) cumprir as obrigações legais aplicáveis e outros requisitos** (por exemplo, obrigações em matéria de proteção de dados, fiscalidade e segurança social, prevenção de riscos e legislação laboral, prevenção de fraudes, denúncia de irregularidades, conservação de registos e obrigações de reporte, exercício de direitos e meios de defesa legais, defesa em processos judiciais, garantia do cumprimento de inspeções governamentais e outros pedidos provenientes de autoridades governamentais ou outras autoridades públicas, resposta a diligências legais, como intimações, cumprimento de obrigações laborais e de segurança social, realização de auditorias e gestão de eventuais queixas ou reclamações internas, etc.).

Relativamente às **categorias especiais de dados pessoais dos colaboradores (incluindo, quando permitido, os dados pessoais relativos a condenações e infrações penais)**, esses dados podem ser tratados pelos Membros do Grupo, quando tal seja necessário para a prossecução das respetivas finalidades (por exemplo, cumprimento de obrigações legais, gestão de recursos humanos, gestão do canal de denúncia de irregularidades, gestão de salários e benefícios, gestão da mobilidade interna, transferências e destacamentos, realização de segmentações agregadas, estatísticas e análises, etc.) e apenas na medida do necessário para efeitos do cumprimento de obrigações e do exercício dos direitos específicos dos Membros do Grupo ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social (artigo 9.º, n.º 2, alínea b), do RGPD), bem como para efeitos de medicina preventiva ou do trabalho, de avaliação da capacidade de trabalho do colaborador, do diagnóstico médico, da prestação de cuidados ou tratamentos de saúde ou de ação social, ou da gestão de sistemas e serviços de saúde ou de ação social (artigo 9.º, n.º 2, alínea h), do RGPD).

- As transferências de dados pessoais de **familiares dos colaboradores** são efetuadas para efeitos da gestão da mobilidade internacional dos colaboradores e da realização de segmentações agregadas, estatísticas e análises, bem como da monitorização do cumprimento do Código de Conduta nos Mercados de Valores Mobiliários ou do cumprimento de políticas semelhantes e das respetivas obrigações, incluindo a aprovação e monitorização de operações de contas pessoais, e para efeitos da gestão dos benefícios sociais relacionados com os direitos dos colaboradores (por exemplo, no contexto de seguros).

- As transferências de dados pessoais de **candidatos atuais e antigos** são efetuadas para efeitos da gestão de atividades de recrutamento nacionais e internacionais (por exemplo, avaliação de candidaturas e tomada de decisões de contratação, comunicação com os candidatos no âmbito do processo de recrutamento e/ou das respetivas candidaturas, etc.).

- As transferências de dados pessoais de **potenciais clientes, consumidores e clientes** (incluindo dos respetivos colaboradores, representantes e/ou agentes, utilizadores autorizados e utilizadores da Web) são efetuadas para as seguintes finalidades: **(a) gerir a relação contratual com os mesmos e prestar os nossos serviços** (por exemplo, emissão de cartões de pagamento, incluindo para utilizadores autorizados de cartões empresariais, disponibilização e gestão dos nossos serviços de pagamento e de banca online, conservação de registos para assegurar o alinhamento da informação entre diferentes jurisdições, celebração de contratos e/ou adoção das medidas necessárias para a respetiva celebração (processos KYC), para fins comerciais e de comunicação, transferências de contas, estabelecimento, renovação, manutenção ou cessação das relações comerciais, disponibilização de acesso a atividades baseadas na Internet e às nossas instalações, manutenção de registos comerciais, realização de auditorias, análises contabilísticas, financeiras e económicas, execução de pagamentos e das respetivas funções contabilísticas, classificação de risco e de crédito/solvência, etc.); **(b) gerir e assegurar a segurança** (por exemplo, proteção da infraestrutura de TI, do equipamento de escritório e de outros

bens, etc.); **(c) gerir as operações comerciais** (por exemplo, conservação de registos dos representantes das empresas ou dos dados de outros contactos, garantia do alinhamento das operações entre diferentes jurisdições, conservação de registos de reuniões e outras relações comerciais, operação e gestão dos sistemas de TI e comunicações, gestão do desenvolvimento de produtos e serviços, melhoria de produtos e serviços, gestão dos ativos da empresa, planeamento estratégico, gestão de projetos, continuidade do negócio, compilação de pistas de auditoria e outras ferramentas de reporte, etc.); **(d) cumprir a legislação aplicável** (por exemplo, obrigações em matéria de proteção de dados e fiscalidade, DMIF e requisitos de adequação e conveniência relativos a produtos de investimento, prevenção de fraudes, combate ao branqueamento de capitais, conservação de registos e obrigações de reporte, exercício de direitos e meios de defesa legais, defesa em litígios ou processos judiciais, garantia do cumprimento de inspeções governamentais e outros pedidos provenientes de autoridades governamentais ou outras autoridades públicas, resposta a diligências legais, como intimações, etc.); e **(e) planear e executar estratégias ou campanhas de marketing** (por exemplo, estudos de mercado, planeamento de campanhas e desenvolvimento de estratégias de marketing, monitorização e reporte do sucesso das campanhas, direcionamento de produtos/serviços (incluindo definição de perfis), quando exista consentimento ou tal seja legalmente permitido, etc.).

Relativamente às **categorias especiais de dados pessoais dos consumidores e clientes (incluindo dos respetivos colaboradores, representantes e/ou agentes)**, **inclusive, quando permitido, os dados pessoais relativos a condenações e infrações penais**, estes dados podem ser tratados pelos Membros do Grupo, quando tal seja necessário para a prossecução das respetivas finalidades (por exemplo, cumprimento de obrigações legais, identificação de informações publicamente disponíveis relativas a práticas de clientes de outras entidades que possam afetar a respetiva relação com a empresa, garantia do alinhamento da informação entre diferentes jurisdições, garantia do cumprimento de inspeções governamentais ou judiciais e outros pedidos provenientes de outras autoridades públicas, etc.) e apenas na medida do necessário para efeitos do cumprimento das obrigações dos Membros do Grupo ou do titular dos dados em matéria de combate ao branqueamento de capitais, prevenção de fraudes, prevenção da criminalidade e domínios conexos (quando tal seja necessário e exigido ou permitido pela legislação aplicável).

- As transferências de dados pessoais de **potenciais e atuais fornecedores, vendedores ou prestadores de serviços** (incluindo dos respetivos colaboradores, representantes e/ou agentes) são efetuadas para as seguintes finalidades: **(a) gerir, em termos gerais, a relação (pré-)contratual com os mesmos ou com a respetiva empresa** (no caso de pessoas coletivas) (por exemplo, realização de verificações dos níveis padrão de qualidade, análise do nível de risco dos prestadores de serviços, análises contabilísticas, financeiras e económicas, adoção das medidas necessárias para a celebração de contratos pertinentes, execução dos contratos em vigor, execução de pagamentos e das respetivas funções contabilísticas, para fins comerciais e de comunicação, estabelecimento, renovação, manutenção ou cessação das relações comerciais, conservação de registos comerciais, etc.); **(b) gerir e assegurar a segurança** (por exemplo, proteção da infraestrutura de TI, do equipamento de escritório e de outros bens, etc.); **(c) gerir as operações comerciais** (por exemplo, operação e gestão dos sistemas de TI e comunicações, gestão do desenvolvimento de produtos e serviços, planeamento estratégico, gestão de projetos, continuidade do negócio, compilação de pistas de auditoria e outras ferramentas de reporte, manutenção de registos relativos às atividades empresariais, orçamentação, gestão e reporte financeiros, comunicações, etc.); e **(d) cumprir a legislação aplicável** (por exemplo, legislação comercial e fiscal, prevenção de fraudes, obrigações em matéria de subcontratação quando efetuada por entidades financeiras, realização de auditorias, cumprimento de inspeções governamentais e outros pedidos provenientes de autoridades governamentais ou outras autoridades públicas, exercício de direitos e meios de defesa legais, defesa em processos judiciais e gestão de eventuais queixas ou reclamações internas, etc.).

- As transferências de dados pessoais de **acionistas** são efetuadas para as seguintes finalidades: **(a) gerir a relação com os acionistas** (por exemplo, para fins comerciais e de comunicação, estabelecimento, renovação, manutenção ou cessação das relações comerciais, gestão das assembleias gerais e dos direitos dos acionistas, pagamento de dividendos, manutenção de registos comerciais, disponibilização de acesso a atividades baseadas na Internet e às instalações, etc.); e **(b) cumprir a legislação aplicável** (por exemplo, legislação comercial, societária, fiscal e de segurança, realização de auditorias, cumprimento de inspeções governamentais e outros pedidos provenientes de autoridades governamentais ou outras autoridades públicas, cumprimento de obrigações em matéria de combate ao branqueamento de capitais, certificações, exercício de direitos e meios de defesa legais, defesa em processos judiciais e gestão de eventuais queixas ou reclamações internas, etc.).

- As transferências de dados pessoais de **utilizadores da Web, utilizadores finais e utilizadores institucionais (incluindo os utilizadores de plataformas, sítios Web ou aplicações relacionados com universidades, emprego e empreendedorismo)** são efetuadas para as seguintes finalidades: **(a) gerir, em termos gerais, a prestação dos serviços** (por exemplo, desenvolvimento e disponibilização de funcionalidades e conteúdos online, gestão de sítios Web, tratamento de pedidos de informação e outras solicitações, prestação de apoio, etc.); **(b) gerir e assegurar a segurança** (por exemplo, proteção da infraestrutura de TI, garantia da segurança e da integridade dos sistemas, servidores e sítios Web, etc.); **(c) gerir as operações comerciais** (por exemplo, garantia do alinhamento das operações entre diferentes jurisdições, conservação de registos de reuniões e outras relações comerciais, melhoria dos processos de gestão de recursos humanos e aquisição de talento a nível global, etc.); **(d) planear e executar estratégias ou campanhas de marketing** (por exemplo, estudos de mercado, planeamento de campanhas e desenvolvimento de estratégias de marketing, monitorização e reporte do sucesso das campanhas, direcionamento de produtos/serviços (incluindo definição de perfis), quando exista consentimento ou tal seja legalmente permitido, etc.); **(e) gerir atividades de recrutamento nacionais e internacionais** (por exemplo, avaliação de candidaturas e tomada de decisões de contratação, comunicação com os candidatos no âmbito do processo de recrutamento e/ou das respetivas candidaturas, etc.); **(f) realizar segmentações agregadas, estatísticas e análises** (por exemplo, compreensão da forma como os serviços são utilizados, melhoria e desenvolvimento das funcionalidades do sítio Web e dos serviços, otimização do desempenho e do apoio disponibilizado, etc.); e **(g) cumprir a legislação aplicável** (por exemplo, legislação comercial, realização de auditorias, cumprimento de inspeções governamentais e outros pedidos provenientes de autoridades governamentais ou outras autoridades públicas, resposta a diligências legais, como intimações, exercício de direitos e meios de defesa legais, defesa em processos judiciais e gestão de eventuais queixas ou reclamações internas, etc.).

Os dados pessoais abrangidos pela presente Política são também transferidos entre os Membros do Grupo, conforme necessário para efeitos de **prestação de uma vasta gama de serviços internos entre os mesmos** (por exemplo, tecnologias e sistemas de TI, serviços administrativos, seleção e gestão de recursos humanos, auditoria interna e conformidade, gestão do canal de denúncia de irregularidades, serviço central de correio para candidaturas e colaboradores, tecnologia de pagamento e serviços de processamento, serviços de autorização e recolha de cartões de crédito, serviços de faturação e definição de preços, destruição de documentos, transporte de documentos, gestão de riscos, aquisição de produtos e/ou serviços, faturação eletrónica, gestão de marketing e comunicações, bem como serviços de gestão e coordenação jurídica em determinadas áreas, como a proteção de dados, etc.).

INFORMAÇÕES ADICIONAIS

O Grupo Santander designou EPD e/ou Responsáveis locais (conforme definição dos termos abaixo), que lideram as equipas locais e asseguram a conformidade local nas diferentes entidades de todo o mundo, integrando igualmente a Equipa de Privacidade do Grupo Santander (também definida abaixo). Em caso de questões relativas às disposições da presente Política, aos seus direitos ao abrigo da mesma ou a quaisquer outras matérias relacionadas com a proteção de dados, pode contactar o EPD/Responsável competente através

do endereço indicado abaixo. O EPD/Responsável irá tratar da questão, encaminhá-la para a pessoa ou o departamento adequado do Grupo Santander ou, quando apropriado, remeter o assunto para a pessoa ou entidade competente.

Atenção: Equipa de Privacidade

E-mail: uma lista dos endereços de e-mail relevantes é apresentada aqui.

Em caso de preocupação relativamente à forma como um Membro do Grupo possa ter tratado os seus dados pessoais, tem à disposição na Parte III um procedimento específico para o tratamento de reclamações (ver **Anexo 2**).

PARTE II: OBRIGAÇÕES DOS MEMBROS DO GRUPO

A Parte II da presente Política está dividida em três secções:

- A Secção A define os princípios fundamentais de proteção de dados, alinhados com a Legislação Europeia em matéria de Proteção de Dados, que um Membro do Grupo deve cumprir.

- A Secção B aborda os compromissos práticos assumidos pelos Membros do Grupo perante as autoridades de controlo competentes no âmbito da presente Política.

- A Secção C descreve os direitos de beneficiários terceiros concedidos pelos Membros do Grupo aos titulares dos dados ao abrigo da Parte II da presente Política.

SECÇÃO A: PRINCÍPIOS FUNDAMENTAIS

REGRA 1 – LICITUDE E JUSTIÇA

Regra 1A – Os Membros do Grupo cumprirão a presente Política e toda a Legislação Local Aplicável em matéria de Proteção de Dados de forma harmonizada.

Enquanto organizações, os Membros do Grupo cumprirão, sem prejuízo do disposto abaixo, toda a legislação aplicável em matéria de dados pessoais (por exemplo, na Europa, é aplicável a Legislação Europeia em matéria de Proteção de Dados) e assegurarão que, sempre que sejam tratados dados pessoais, esse tratamento será efetuado em conformidade com a presente Política e com a Legislação Local Aplicável em matéria de Proteção de Dados.

Sempre que a presente Política seja aplicável e:

- não exista uma Legislação Local Aplicável em matéria de Proteção de Dados, ou essa legislação não cumpra os padrões estabelecidos pelas Regras da presente Política, os Membros do Grupo tratarão os dados pessoais que estão sujeitos à presente Política em conformidade com as Regras nela estabelecidas;

- a Legislação Local Aplicável em matéria de Proteção de Dados imponha um nível de proteção mais elevado do que o nível previsto na presente Política, prevalecerá o nível de proteção mais elevado sobre a presente Política, desde que os direitos e as obrigações previstos na presente Política continuem a ser respeitados; ou

- a Legislação Local Aplicável em matéria de Proteção de Dados impeça os Membros do Grupo de cumprirem a presente Política, ou tenha um efeito substancial na respetiva capacidade de cumprir as obrigações nela previstas, os Membros do Grupo seguirão o procedimento estabelecido na Regra 13.

Regra 1B – Os Membros do Grupo assegurarão que o tratamento de dados pessoais é lícito e justo e que, sempre que exigido, existe um fundamento jurídico para o tratamento dos mesmos.

Os Membros do Grupo assegurarão que o tratamento de dados pessoais é lícito e justo e que, sempre que exigido, existe um fundamento jurídico para o tratamento dos mesmos. Em conformidade com a Legislação Europeia em matéria de Proteção de Dados, os Membros do Grupo apenas tratarão dados pessoais quando:

- o titular dos dados der o seu consentimento para o tratamento dos seus dados pessoais e esse consentimento cumprir os requisitos previstos na Legislação Europeia em matéria de Proteção de Dados (isto é, ser dado de forma livre, específica, informada e inequívoca); ou

- o tratamento for necessário para a execução de um contrato no qual o titular dos dados seja parte integrante ou para a realização de diligências pré-contratuais a pedido do titular dos dados; ou

- o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o Membro do Grupo esteja sujeito (desde que a referida obrigação cumpra os requisitos previstos na Regra 13 da presente Política, quando aplicável); ou

- o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou

- o tratamento for necessário para o desempenho de funções de interesse público ou para o exercício da autoridade pública conferida a um Membro do Grupo (desde que as referidas funções estejam previstas na lei e que esta cumpra os requisitos previstos na Regra 13 da presente Política, quando aplicável); ou

- o tratamento for necessário para efeitos dos interesses legítimos prosseguidos por um Membro do Grupo ou por um terceiro, exceto quando esses interesses sejam prevalecidos pelos interesses ou pelos direitos e liberdades fundamentais do titular dos dados.

Sempre que o tratamento de dados pessoais diga respeito a condenações e infrações penais ou a medidas de segurança conexas, os Membros do Grupo não efetuarão o referido tratamento, salvo sob o controlo de uma autoridade pública ou quando o tratamento seja autorizado por uma lei que preveja garantias adequadas para os direitos e as liberdades dos titulares dos dados, em conformidade com os fundamentos jurídicos acima referidos.

Regra 1C – Sem prejuízo da Regra 1B acima, é proibido o tratamento de categorias especiais de dados pessoais, exceto em caso de derrogação, como sucede com as categorias previstas na Legislação Europeia em matéria de Proteção de Dados.

O tratamento de categorias especiais de dados pessoais só é permitido com base em determinados fundamentos:

- o Membro do Grupo obteve o consentimento explícito para o tratamento de quaisquer categorias especiais dos dados pessoais do titular dos dados associado a uma ou mais finalidades específicas, salvo quando a lei determine que a proibição do tratamento de dados de categorias especiais não possa ser anulada pelo titular dos dados; ou

- o tratamento é necessário para efeitos do cumprimento de obrigações e do exercício dos direitos específicos do Membro do Grupo ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que seja autorizado por lei ou por uma convenção coletiva, nos termos da lei, que antecipe um conjunto de garantias adequadas para os direitos fundamentais e os interesses dos titulares dos dados; ou

- o tratamento é necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, quando o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento; ou

- o tratamento é efetuado no âmbito das atividades legítimas de uma fundação, associação ou qualquer outro organismo sem fins lucrativos, com fins políticos, filosóficos, religiosos ou sindicais e com garantias adequadas e desde que o tratamento diga respeito exclusivamente aos membros ou antigos membros do referido organismo, ou a pessoas que com ele mantenham contactos regulares relacionados com as respetivas finalidades, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos titulares dos dados; ou

- o tratamento diz respeito a dados pessoais que tenham sido manifestamente tornados públicos pelo titular dos dados; ou

- o tratamento é necessário para a declaração, o exercício ou a defesa de direitos em processos judiciais, ou sempre que os tribunais atuem no exercício da sua capacidade jurídica; ou

- o tratamento é necessário por motivos de interesse público significativo, com base numa lei que seja proporcional ao objetivo visado, respeite a essência da proteção de dados e preveja medidas adequadas e específicas para salvaguardar os direitos fundamentais e os interesses do titular dos dados; ou

- o tratamento é necessário para efeitos de medicina preventiva ou do trabalho, de avaliação da capacidade de trabalho do colaborador, do diagnóstico médico, da prestação de cuidados ou tratamentos de saúde ou de ação social, ou da gestão de sistemas e serviços de saúde ou de ação social, com base numa lei que determine que o tratamento é efetuado por ou sob a sua responsabilidade de um profissional sujeito ao dever de sigilo nos termos da lei ou de normas estabelecidas pelas autoridades nacionais competentes; ou

- o tratamento é necessário por motivos de interesse público no domínio da saúde pública, com base numa lei que prevê medidas adequadas e específicas para salvaguardar os direitos e as liberdades dos titulares dos dados, em particular o dever de sigilo profissional; ou

- o tratamento é necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, com base numa lei que será proporcional ao objetivo visado, respeite a essência do direito à proteção de dados e preveja medidas adequadas e específicas para salvaguardar os direitos fundamentais e os interesses do titular dos dados.

Regra 1D – Os Membros do Grupo irão avaliar o impacto de qualquer tratamento de dados pessoais que implique riscos elevados para os direitos e as liberdades dos titulares dos dados.

As Entidades Exportadoras, quando atuem na qualidade de responsáveis pelo tratamento, irão avaliar a necessidade e a proporcionalidade de qualquer novo tratamento de dados pessoais e, caso este implique um risco elevado para os direitos e as liberdades dos titulares dos dados, irão realizar uma avaliação de impacto sobre a proteção de dados, em conformidade com a Legislação Europeia em matéria de Proteção de Dados. Caso a avaliação de impacto sobre a proteção de dados indique que o tratamento resultará num risco elevado para os titulares dos dados e na ausência de medidas adotadas para mitigar o mesmo, as Entidades Exportadoras serão obrigadas a consultar as autoridades de controlo competentes antes de iniciarem o tratamento.

REGRA 2 – ASSEGURAR A TRANSPARÊNCIA E O TRATAMENTO DE DADOS PESSOAIS APENAS PARA UMA DETERMINADA FINALIDADE

Regra 2A – Os Membros do Grupo irão informar os titulares dos dados sobre a forma como os dados serão tratados.

Os Membros do Grupo assegurarão que os titulares dos dados sejam sempre informados, de forma clara e compreensível (normalmente através de uma declaração de tratamento justo), sobre a forma como serão tratados os respetivos dados pessoais. O Membro do Grupo competente irá fornecer as informações exigidas pela Legislação Europeia em matéria de Proteção de Dados, incluindo, pelo menos:

- a identidade e os dados de contacto do responsável pelo tratamento, incluindo, quando aplicável, os dados de contacto do encarregado da proteção de dados e do representante;

- a finalidade e o fundamento jurídico do tratamento, incluindo uma explicação sobre qualquer tratamento baseado em interesses legítimos e sobre quaisquer finalidades compatíveis novas ou diferentes;

- os destinatários ou as categorias de destinatários dos dados pessoais;

- informações sobre as garantias aplicáveis à proteção dos dados pessoais quando estes são objeto de transferências internacionais e informações sobre a forma de aceder às referidas garantias ou obter uma cópia das mesmas. No caso de transferências de dados pessoais entre uma Entidade Exportadora e uma Entidade Importadora com base na presente Política, as informações fornecidas incluirão uma referência à presente Política e à forma de aceder à mesma;

- o período durante o qual os dados pessoais serão conservados ou, caso tal não seja possível, os critérios utilizados para determinar o período em questão;

- informações sobre os direitos dos titulares dos dados, incluindo os direitos de acesso, retificação, apagamento, limitação, oposição, portabilidade, retirada de consentimento (nos casos em que o tratamento se baseie no consentimento), bem como o direito de apresentar uma reclamação junto de uma autoridade de controlo;

- se o fornecimento das informações constitui uma obrigação legal ou contratual e quais as consequências da não disponibilização dos dados pessoais em tais circunstâncias; e

- informações sobre a existência de decisões automatizadas, incluindo a definição de perfis, e, pelo menos nos casos em que as referidas decisões produzam efeitos jurídicos relativamente ao titular dos dados ou o afetem de forma semelhante e significativa, ou se baseiem em categorias especiais de dados pessoais, e informações úteis sobre a lógica subjacente, bem como sobre a importância e as consequências previstas do tratamento para o titular dos dados.

Os requisitos da Legislação Local Aplicável em matéria de Proteção de Dados do local onde os dados pessoais são recolhidos determinam se é necessário fornecer informações adicionais aos titulares dos dados.

Estas informações serão fornecidas quando os dados pessoais forem obtidos pelos Membros do Grupo junto do titular dos dados ou dentro de um prazo permitido, de outra forma, pela Legislação Europeia em matéria de Proteção de Dados.

Sempre que os Membros do Grupo obtiverem dados pessoais de um titular dos dados a partir de uma fonte distinta do referido titular, o Membro do Grupo competente fornecerá as informações ao titular dos dados, juntamente com informações sobre a fonte e as categorias de dados pessoais recebidos de terceiros, nos seguintes prazos:

- num prazo razoável após a recolha dos dados pessoais, mas, o mais tardar, no prazo de um (1) mês;

- se os dados pessoais se destinarem a ser tratados para efeitos de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação dirigida ao titular dos dados; ou

- se os dados pessoais tiverem de ser divulgados a um terceiro, o mais tardar no momento da primeira divulgação dos mesmos.

Os Membros do Grupo cumprirão a presente Regra 2A, salvo quando a não prestação das informações seja especificamente permitida pela Legislação Europeia em matéria de Proteção de Dados.

Regra 2B – Os Membros do Grupo só irão obter e tratar dados pessoais para finalidades que sejam do conhecimento do titular dos dados, ou que sejam compatíveis com as respetivas expectativas e pertinentes para os Membros do Grupo.

A Regra 1A estabelece que os Membros do Grupo cumprirão, na íntegra, a legislação aplicável relativa ao tratamento de dados pessoais (desde que a referida legislação cumpra os requisitos previstos na Regra 13 da presente Política, quando aplicável). Tal significa que os Membros do Grupo irão recolher dados pessoais para finalidades específicas, explícitas e legítimas e não irão proceder ao tratamento posterior dos mesmos de forma incompatível com as finalidades definidas.

Os Membros do Grupo irão identificar e dar a conhecer as finalidades para as quais os dados pessoais serão tratados (incluindo as utilizações secundárias e as divulgações dos dados) em conformidade com a Regra 2A.

Regra 2C – Os Membros do Grupo só poderão tratar dados pessoais para uma finalidade diferente ou nova se essa finalidade for compatível com a finalidade de recolha dos dados.

Sempre que um Membro do Grupo recolher dados pessoais para uma finalidade específica em conformidade com a Regra 2A (conforme comunicada ao titular dos dados através da respetiva declaração de tratamento justo) e conforme descrito na Regra 2B, e posteriormente pretender tratar esses dados pessoais para uma finalidade diferente ou nova, não procederá ao tratamento posterior dos dados pessoais de forma incompatível com a finalidade para a qual foram recolhidos, salvo se o tratamento posterior se basear no consentimento do titular dos dados ou se for exigido por lei (desde que a lei cumpra os requisitos previstos na Regra 13 da presente Política, quando aplicável).

REGRA 3 – ASSEGURAR A QUALIDADE DOS DADOS

Regra 3A – Os Membros do Grupo manterão os dados pessoais exatos e atualizados.

A fim de assegurar que os dados pessoais detidos pelos Membros do Grupo são exatos e se mantêm atualizados, os Membros do Grupo incentivarão ativamente os titulares dos dados a informá-los sempre que os dados pessoais sofrerem alterações. Os Membros do Grupo adotarão medidas razoáveis para assegurar que os dados pessoais inexatos, tendo em conta as finalidades para as quais são tratados, são prontamente apagados ou retificados.

Regra 3B – Os Membros do Grupo só irão conservar os dados pessoais durante o período necessário para as finalidades para as quais são tratados.

Os Membros do Grupo cumprirão a regulamentação aplicável a cada Membro do Grupo, bem como as políticas e os procedimentos de conservação de registos do Grupo Santander, conforme revistos e atualizados

periodicamente. Entre outros aspetos, isso significa que os Membros do Grupo apagam ou bloqueiam, consoante o caso, os dados pessoais que deixam de ser necessários para a finalidade para a qual são recolhidos e posteriormente tratados.

Regra 3C – Os Membros do Grupo só irão tratar dados pessoais que sejam adequados, pertinentes e limitados ao que é necessário para as finalidades para as quais são tratados.

Os Membros do Grupo só irão tratar os dados pessoais necessários para a prossecução das finalidades para as quais são tratados.

REGRA 4 – ADOTAR MEDIDAS DE SEGURANÇA ADEQUADAS

Regra 4A – Os Membros do Grupo cumprirão as políticas de segurança de TI do Grupo Santander.

Os Membros do Grupo irão implementar medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição ou perda acidental ou ilícita, a alteração, a divulgação ou o acesso não autorizados, em especial quando o tratamento implique a transmissão de dados pessoais através de uma rede, e contra quaisquer outras formas ilícitas de tratamento. Para o efeito, os Membros do Grupo cumprirão os requisitos previstos nas políticas de segurança em vigor no Grupo Santander, conforme revistas e atualizadas periodicamente, bem como quaisquer outros procedimentos de segurança relevantes para uma determinada área ou função de negócio. Tendo em conta as técnicas mais avançadas e os custos da sua implementação, essas medidas assegurarão um nível de segurança adequado aos riscos apresentados pelo tratamento e pela natureza dos dados a proteger.

Regra 4B – Os Membros do Grupo implementaram uma política de notificação de violação de dados.

Os Membros do Grupo implementaram procedimentos de resposta a violações de dados pessoais (conforme revistos e atualizados periodicamente) que estabelecem o procedimento a seguir em caso de uma violação de segurança que provoque a destruição, a perda, a alteração, a divulgação não autorizada ou o acesso não autorizado, acidental ou ilícito, a dados pessoais transmitidos, conservados ou de outra forma tratados (uma «**Violação de Dados Pessoais**»).

Em particular, em caso de Violação de Dados Pessoais, a pessoa do Membro do Grupo que tiver conhecimento da mesma notificá-la-á, sem demora injustificada, às seguintes entidades:

- o EPD ou Responsável competente, através da Função de Controlo do Risco Operacional (quando aplicável);
- o Membro do Grupo que atue na qualidade de responsável pelo tratamento, quando o Membro do Grupo em causa atuar como subcontratante; e
- o Membro Responsável pelas RVE.

O EPD ou Responsável competente avaliará, com o apoio do Gabinete Corporativo de Proteção de Dados, sempre que necessário, se a Violação de Dados Pessoais deve ser notificada à autoridade de controlo competente. Se assim for, o EPD ou Responsável competente, conforme o caso, procederá à notificação da Violação de Dados Pessoais junto da autoridade de controlo competente dentro do prazo exigido (de acordo com a Legislação Europeia em matéria de Proteção de Dados, sem demora injustificada e sempre que possível, o prazo será 72 horas, o mais tardar, após a tomada de conhecimento da referida violação).

Os titulares dos dados serão igualmente notificados sem demora injustificada nos casos em que seja provável que a Violação de Dados Pessoais resulte num risco elevado para os respetivos direitos e liberdades, salvo quando a referida notificação não seja exigida pela Legislação Europeia em matéria de Proteção de Dados.

Em conformidade com o acima exposto, as Violações de Dados Pessoais sofridas pelos Membros do Grupo, incluindo os factos, os efeitos dos incidentes e as medidas corretivas adotadas, serão igualmente registadas no Heracles, o registo de incidentes de segurança (incluindo Violações de Dados Pessoais) do Grupo Santander, o qual será disponibilizado à autoridade de controlo competente mediante pedido.

Regra 4C – Os Membros do Grupo assegurarão que os prestadores de serviços e outras entidades que tratem dados pessoais em seu nome também adotam medidas de segurança adequadas e equivalentes.

Os Membros do Grupo que recorrerem a um prestador de serviços (na qualidade de subcontratante) que tenha acesso aos dados pessoais dos titulares dos dados (por exemplo, um prestador de serviços de processamento salarial) imporão ao subcontratante, por escrito, um conjunto de obrigações contratuais que cumpram os requisitos da Legislação Europeia em matéria de Proteção de Dados, sob a forma de um acordo vinculativo de tratamento de dados. O referido acordo irá prever, pelo menos, o seguinte:

- O objeto e a duração do tratamento, a natureza e a finalidade do mesmo, o tipo de dados pessoais e as categorias de titulares dos dados;

- As obrigações e os direitos do responsável pelo tratamento;

- As seguintes obrigações da entidade que atua na qualidade de subcontratante:

    - Tratar os dados pessoais apenas com base em instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados pessoais para um país terceiro ou uma organização internacional, salvo se tal for exigido por uma lei a que o subcontratante esteja sujeito (desde que a referida lei cumpra os requisitos previstos na Regra 13 da presente Política, quando aplicável). Nesse caso, o subcontratante informará o responsável pelo tratamento do requisito legal antes de proceder ao tratamento, salvo se a lei proibir tal informação por motivos relevantes de interesse público;

    - Assegurar que as pessoas autorizadas a tratar os dados pessoais se comprometem a respeitar a confidencialidade ou estão sujeitas a uma obrigação legal adequada de confidencialidade;

    - Implementar medidas técnicas e organizativas adequadas para assegurar um nível de segurança apropriado aos riscos inerentes ao tratamento dos dados pessoais;

    - Não recorrer a outro subcontratante para o tratamento dos dados pessoais sem a autorização prévia, específica ou geral, por escrito, do responsável pelo tratamento e celebrar, consoante o caso, um acordo escrito com o subcontratante ulterior que imponha as mesmas obrigações em matéria de proteção de dados previstas no contrato ou noutro ato jurídico celebrado entre o responsável pelo tratamento e o subcontratante (assegurando, em especial, garantias suficientes para a implementação de medidas técnicas e organizativas adequadas, de modo que o tratamento cumpra os requisitos da Legislação Europeia em matéria de Proteção de Dados);

    - Tendo em conta a natureza do tratamento, prestar assistência ao responsável pelo tratamento, através de medidas técnicas e organizativas adequadas, na medida do possível, para que este

possa cumprir a sua obrigação de responder aos pedidos de exercício dos direitos do titular dos dados (descritos mais detalhadamente na Regra 5 abaixo);

- Prestar assistência ao responsável pelo tratamento para assegurar o cumprimento das obrigações relacionadas com a implementação de medidas de segurança adequadas e a realização de avaliações de impacto sobre a proteção de dados e de consultas conexas junto das autoridades de controlo competentes, bem como das obrigações de notificação de Violações de Dados Pessoais junto das autoridades de controlo competentes e dos titulares dos dados (quando aplicável);

- À escolha do responsável pelo tratamento, apagar ou devolver ao responsável pelo tratamento todos os dados pessoais após o termo da prestação dos serviços relacionados com o tratamento e apagar as cópias existentes, salvo quando a conservação dos dados pessoais seja exigida por lei;

- Disponibilizar ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações enquanto subcontratante e permitir e contribuir para auditorias, incluindo inspeções, realizadas pelo responsável pelo tratamento ou por outro auditor mandatado por este; e

- Informar imediatamente o responsável pelo tratamento se, na sua opinião, uma instrução violar a lei.

REGRA 5 – RESPEITAR OS DIREITOS DOS TITULARES DOS DADOS

Regra 5 – Os Membros do Grupo tratarão os pedidos de exercício de direitos dos titulares dos dados em matéria de proteção de dados (incluindo os direitos de acesso, retificação, apagamento, limitação ou transmissão dos dados pessoais, oposição ao tratamento dos mesmos, bem como a retirada de consentimento).

Mediante pedido, os titulares dos dados têm direito a exercer os seguintes direitos, nos termos da Legislação Europeia em matéria de Proteção de Dados:

- direito de acesso, que consiste na prestação de informações sobre os dados pessoais disponíveis relativos ao titular dos dados e na confirmação de tratamento dos respetivos dados pessoais;

- direito de retificação, ao abrigo do qual o titular dos dados tem o direito de obter a retificação de quaisquer dados pessoais inexatos ou incompletos;

- direito ao apagamento ou «direito a ser esquecido», ao abrigo do qual o titular dos dados tem o direito de obter o apagamento dos seus dados pessoais quando se verifiquem determinadas circunstâncias (como as disposições previstas no artigo 17.º do RGPD);

- direito à limitação do tratamento, ao abrigo do qual o titular dos dados tem o direito de solicitar a limitação do tratamento dos seus dados pessoais quando se verifiquem determinadas circunstâncias (como as disposições previstas no artigo 18.º do RGPD);

- direito de exigir que cada destinatário a quem os dados pessoais tenham sido divulgados seja notificado de eventuais retificações ou apagamentos dos dados pessoais ou limitações do tratamento, salvo se tal se revelar impossível ou implicar um esforço desproporcionado. O titular dos dados pode também pedir para ser informado sobre os referidos destinatários;

- direito de portabilidade dos dados, ao abrigo do qual o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, tendo também o direito de transmitir esses dados a outro responsável pelo tratamento;

- direito de oposição, ao abrigo do qual o titular dos dados tem o direito de se opor ao tratamento dos seus dados pessoais para uma finalidade específica, incluindo o tratamento para efeitos de comercialização direta e definição de perfis, na medida em que esta esteja relacionada com a referida comercialização;

- direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos jurídicos na sua esfera jurídica ou o afete de forma significativa (quando aplicável); e

- direito de retirar, a qualquer momento, o consentimento dado para um tratamento específico.

REGRA 6 – ASSEGURAR UMA PROTEÇÃO ADEQUADA ÀS TRANSFERÊNCIAS E TRANSFERÊNCIAS ULTERIORES

Regra 6 – Os Membros do Grupo não transferirão dados pessoais para terceiros situados fora da Europa sem assegurar uma proteção adequada dos dados pessoais, em conformidade com os padrões estabelecidos na presente Política e a Legislação Europeia em matéria de Proteção de Dados.

As transferências e as transferências ulteriores de dados pessoais efetuadas por Membros do Grupo sujeitos à Legislação Europeia em matéria de Proteção de Dados para terceiros situados fora da Europa não são permitidas sem a adoção de medidas adequadas, conforme exigido pela Legislação Europeia em matéria de Proteção de Dados.

Estas medidas podem incluir, entre outras:

- confirmar que o terceiro está estabelecido num país que a Comissão Europeia tenha considerado assegurar um nível de proteção adequado dos dados pessoais transferidos; ou

- celebrar cláusulas contratuais-tipo adequadas ou recorrer a outros mecanismos previstos na Legislação Europeia em matéria de Proteção de Dados; ou

- assegurar que a transferência é necessária: (i) para a execução de um contrato entre o titular dos dados e o Membro do Grupo que efetua a transferência, ou para a aplicação de medidas pré-contratuais adotadas a pedido do titular dos dados; (ii) para a celebração ou a execução de um contrato celebrado, no interesse do titular dos dados, entre o Membro do Grupo que efetua a transferência e outro terceiro; (iii) por motivos importantes de interesse público reconhecidos pelo direito da União ou pelo direito do Estado-Membro a que o responsável pelo tratamento está sujeito; (iv) para o estabelecimento, o exercício ou a defesa de direitos em processos judiciais; (v) para a proteção dos interesses vitais do titular dos dados ou de outra pessoa singular, quando o titular dos dados estiver incapaz de dar o seu consentimento; ou (vi) para a obtenção do consentimento explícito dos titulares dos dados, após estes terem sido informados dos possíveis riscos da referida transferência decorrentes da inexistência de uma decisão de adequação e de garantias adequadas.

SECÇÃO B: COMPROMISSOS PRÁTICOS

REGRA 7 – CONFORMIDADE E RESPONSABILIZAÇÃO

Regra 7A – Os Membros do Grupo serão responsáveis pelo cumprimento da presente Política e serão capazes de demonstrar esse cumprimento, dispondo de pessoal e apoio adequados para assegurar e supervisionar o cumprimento da presente Política em toda a organização.

O Grupo Santander dispõe de uma estrutura organizacional de proteção da privacidade responsável por decidir, coordenar, implementar e supervisionar qualquer atividade que possa ter lugar no Grupo Santander em matéria de proteção de dados (a «**Equipa de Privacidade**»). A estrutura de proteção da privacidade do Grupo Santander é composta por:

- **Gabinete Corporativo de Proteção de Dados:** órgão corporativo responsável por definir os critérios gerais e elaborar as políticas corporativas aplicáveis em matéria de proteção de dados. Em conjunto com a equipa de Risco Não Financeiro, constitui a segunda linha global de defesa (2LoD), responsável pela supervisão da gestão de atividades de privacidade desenvolvidas pela primeira linha de defesa (1LoD) e por assegurar uma gestão adequada do risco em conformidade com a apetência pelo risco do Grupo Santander.

  Enquanto 2LoD Global, o Gabinete Corporativo de Proteção de Dados e a equipa de Risco Não Financeiro assumem um conjunto de funções relativas a todas as entidades do Grupo Santander sujeitas à Legislação Europeia em matéria de Proteção de Dados, incluindo, principalmente:

  - Monitorização e controlo da conformidade: (i) monitorizar a conformidade do Grupo Santander em matéria de proteção de dados; (ii) apresentar informação consolidada à gestão de topo do Grupo Santander; (iii) atuar como ponto de contacto global, através dos diferentes EPD locais (ou figura equivalente), junto das autoridades de controlo competentes; (iv) realizar análises de impacto, em conjunto com as funções de negócio e apoio relevantes, relativas a incidentes de segurança a nível global; (v) realizar análises e elaborar relatórios sobre os riscos globais em matéria de proteção de dados; e (vi) facilitar a definição de critérios corporativos e atuar como ponto de contacto na organização junto dos EPD/Responsáveis das entidades (ver abaixo).

  - Função de apoio aos EPD e Responsáveis do Grupo Santander (unidades/entidades corporativas e entidades locais), prestando principalmente aconselhamento especializado em matéria regulamentar e apoio ao desempenho das funções locais de proteção da privacidade.

- **Estrutura e Governação**

  - **Banco Santander (Sociedade):** duas figuras principais prestam apoio e reportam ao Gabinete Corporativo de Proteção de Dados:

    - **EPD do Banco Santander** (formalmente designado perante a autoridade de controlo espanhola): as funções que o EPD desempenha, de forma independente, na sociedade-mãe limitam-se às funções previstas no RGPD que exigem, entre outros aspetos, a respetiva participação no diálogo junto da autoridade de controlo espanhola. Sem prejuízo das obrigações de reporte e apoio do EPD perante o Gabinete Corporativo de Proteção de Dados, o EPD reporta diretamente ao nível de gestão mais elevado do Banco Santander.

    - **Unidades corporativas:** unidades designadas em toda a organização. As suas principais funções e responsabilidades consistem em: (a) executar e resolver, em primeira

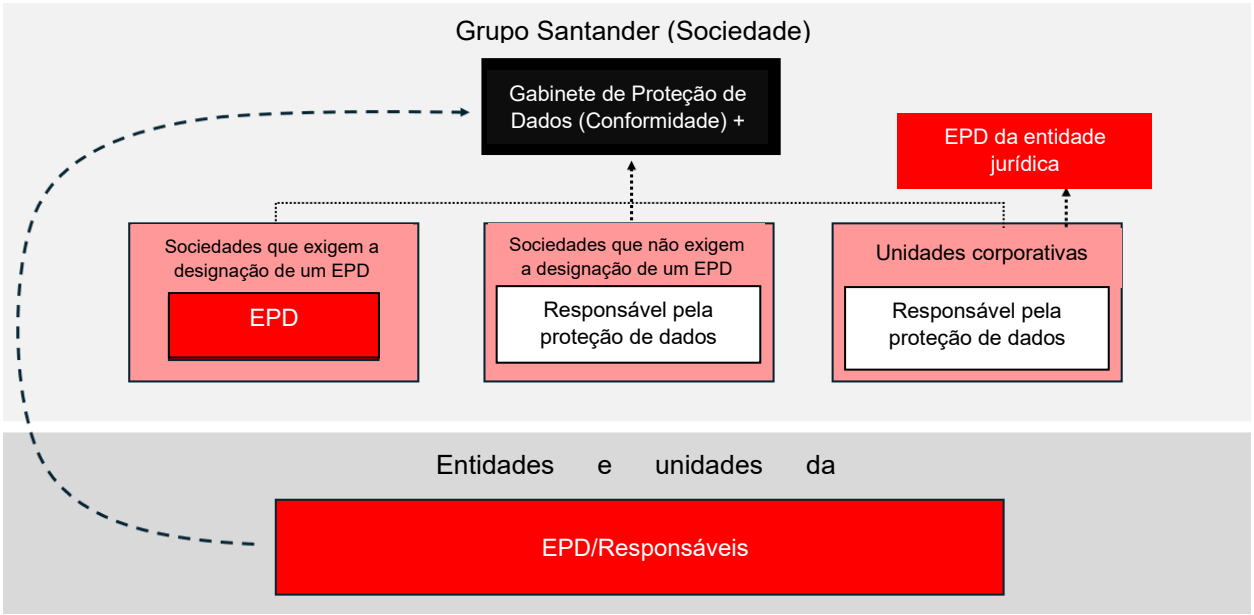
instância, as questões relacionadas com dados pessoais; (b) informar e aconselhar os responsáveis pelo tratamento, os subcontratantes e os colaboradores sobre a forma de cumprir a regulamentação aplicável em matéria de proteção de dados; (c) monitorizar a conformidade com a regulamentação em matéria de proteção de dados; (d) atuar como ponto de contacto interno de primeira linha; (e) encaminhar consultas e pedidos de apoio para o Gabinete Corporativo de Proteção de Dados e reportar indicadores de gestão.

- **Unidades locais:** também existem duas figuras que reportam ao Gabinete Corporativo de Proteção de Dados:

  - **EPD (ou figura local equivalente):** sempre que exigido pela Legislação Local Aplicável em matéria de Proteção de Dados, é designado um EPD (ou figura local equivalente). As suas principais funções e responsabilidades podem incluir: (a) atuar como ponto de contacto junto da autoridade de controlo competente e das partes interessadas; (b) cooperar com a autoridade de controlo competente; (c) prestar aconselhamento em matéria de proteção de dados; (d) monitorizar e supervisionar; (e) ministrar formação; (f) prestar aconselhamento ao nível das avaliações de impacto sobre a proteção de dados; (g) realizar consultas prévias junto da autoridade de controlo competente; (h) supervisionar os registos das atividades de tratamento; (i) prestar aconselhamento sobre a notificação de Violações de Dados Pessoais; (j) prestar aconselhamento sobre a gestão de terceiros; e (k) supervisionar o exercício dos direitos dos titulares dos dados.

  - **Responsáveis ou figura local equivalente (por exemplo, responsável pela privacidade):** sempre que a Legislação Local Aplicável em matéria de Proteção de Dados não exija a designação de um EPD ou quando, devido à dimensão e/ou complexidade de uma entidade, seja necessário um número elevado de EPD ou figuras locais equivalentes, o Gabinete Corporativo de Proteção de Dados pode ser apoiado e receber comunicações dos Responsáveis locais ou de figuras locais equivalentes (por exemplo, responsável pela privacidade). As suas funções e responsabilidades são muito semelhantes às funções e responsabilidades dos EPD ou de figuras locais equivalentes, com exceção das comunicações mantidas com as autoridades de controlo (nas quais não intervêm).

Segue-se um diagrama que apresenta a estrutura organizacional e as relações entre as figuras acima referidas responsáveis pela proteção de dados no Grupo Santander:



Regra 7B – Os Membros do Grupo implementarão medidas técnicas e organizativas adequadas, desde a conceção e por defeito, para permitir e facilitar, na prática, o cumprimento da presente Política.

Tendo em conta as técnicas mais avançadas, os custos de implementação e o âmbito, a natureza, o contexto e as finalidades do tratamento, os Membros do Grupo implementarão medidas técnicas e organizativas adequadas que cumpram os princípios de proteção de dados desde a conceção e por defeito, conforme exigido pela Legislação Europeia em matéria de Proteção de Dados. Os Membros do Grupo irão integrar as referidas medidas no tratamento ao determinar os meios de tratamento e no momento do próprio tratamento, a fim de facilitar a proteção dos dados pessoais em tratamento e assegurar que, por defeito, apenas são tratados os dados pessoais necessários para cada finalidade específica do tratamento.

Regra 7C – Os Membros do Grupo que tratarem dados pessoais manterão um registo escrito (incluindo em formato eletrónico) das respetivas atividades de tratamento e disponibilizá-lo-ão às autoridades de controlo competentes, mediante pedido.

Os registos de tratamento de dados mantidos pelos Membros do Grupo, quando estes atuam na qualidade de responsáveis pelo tratamento, contêm:

- o nome e os dados de contacto do Membro do Grupo e, quando aplicável, do responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;
- as finalidades para as quais são tratados os dados pessoais;
- a descrição das categorias de titulares dos dados cujos dados pessoais são tratados e dos dados pessoais tratados;
- as categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários de países terceiros ou organizações internacionais;
- informações sobre o país terceiro ou os países terceiros para os quais são transferidos os dados pessoais, incluindo a identificação do país terceiro ou da organização internacional em causa e a

documentação das garantias adequadas implementadas para legitimar as referidas transferências (salvo se o país tiver sido declarado adequado nos termos da Legislação Europeia em matéria de Proteção de Dados);

- sempre que possível, o período durante o qual serão conservados os dados pessoais; e
- sempre que possível, uma descrição geral das medidas técnicas e organizativas de segurança utilizadas para proteger os dados pessoais.

Os registos de tratamento de dados mantidos pelos Membros do Grupo, quando estes atuam na qualidade de subcontratantes de um Membro do Grupo que age como responsável pelo tratamento, contêm:

- o nome e os dados de contacto do Membro do Grupo e de cada responsável pelo tratamento em nome do qual o subcontratante atua e, quando aplicável, do representante do responsável pelo tratamento ou do subcontratante e do encarregado da proteção de dados;
- as categorias de atividades de tratamento efetuadas por conta de cada responsável pelo tratamento;
- informações sobre o país terceiro ou os países terceiros para os quais são transferidos os dados pessoais, incluindo a identificação do país terceiro ou da organização internacional em causa e a documentação das garantias adequadas implementadas para legitimar as referidas transferências (salvo se o país tiver sido declarado adequado nos termos da Legislação Europeia em matéria de Proteção de Dados); e
- sempre que possível, uma descrição geral das medidas técnicas e organizativas de segurança utilizadas para proteger os dados pessoais.

Os registos de tratamento de dados mantidos pelos Membros do Grupo serão conservados por escrito, incluindo em formato eletrónico, e disponibilizados às autoridades de controlo competentes, mediante pedido.

REGRA 8 – FORMAÇÃO

Regra 8 – Os Membros do Grupo irão proporcionar formação adequada aos colaboradores que tiverem acesso permanente ou regular a dados pessoais e/ou estiverem envolvidos no tratamento dos mesmos ou no desenvolvimento de ferramentas utilizadas para o respetivo tratamento.

Os Membros do Grupo irão proporcionar formação adequada e atualizada aos colaboradores que tiverem acesso permanente ou regular a dados pessoais e/ou estiverem envolvidos no tratamento dos mesmos ou no desenvolvimento de ferramentas utilizadas para o respetivo tratamento. Esta formação será ministrada, pelo menos, uma vez de dois em dois anos e irá abranger, entre outros aspetos, os procedimentos de gestão de pedidos de acesso a dados pessoais apresentados por autoridades públicas.

REGRA 9 – AUDITORIA

Regra 9 – Os Membros do Grupo cumprirão o Programa de Auditoria definido no Anexo 1.

Os Membros do Grupo cumprirão o Programa de Auditoria através da realização de auditorias internas periódicas e permitindo a realização de auditorias externas, quando exigido, em conformidade com o processo formal de avaliação previsto no Programa de Auditoria. Os resultados das auditorias serão comunicados em conformidade com o Anexo 1.

REGRA 10 – TRATAMENTO DE RECLAMAÇÕES

Regra 10 – Os Membros do Grupo cumprirão o Procedimento de Tratamento de Reclamações definido no Anexo 2.

Os Membros do Grupo cumprirão o Procedimento de Tratamento de Reclamações definido no Anexo 2, a fim de tratar de forma adequada as reclamações dos titulares dos dados e salvaguardar o tratamento de dados pessoais pelos Membros do Grupo. Os Membros do Grupo irão também assegurar o exercício dos direitos de beneficiários terceiros, conforme previsto na Secção C da presente Política.

REGRA 11 – COOPERAÇÃO COM AS AUTORIDADES DE CONTROLO COMPETENTES

Regra 11 – Os Membros do Grupo cumprirão o Procedimento de Cooperação definido no Anexo 3.

Os Membros do Grupo cumprirão o Procedimento de Cooperação definido no Anexo 3 e cooperarão com as autoridades de controlo competentes, aceitando ser objeto de auditorias e inspeções das mesmas (incluindo no local, sempre que necessário) no âmbito da presente Política, além de terem em consideração os respetivos pareceres e respeitarem as decisões apresentadas sobre eventuais questões relacionadas com a presente Política.

REGRA 12 – ATUALIZAÇÃO DAS REGRAS

Regra 12 – Os Membros do Grupo cumprirão o Procedimento de Atualização definido no Anexo 4.

Os Membros do Grupo cumprirão o Procedimento de Atualização definido no Anexo 4 e comunicarão, sem demora injustificada, qualquer atualização da presente Política e da lista de Membros do Grupo às autoridades de controlo competentes, aos titulares dos dados em causa e aos Membros do Grupo, conforme necessário.

REGRA 13 – ATUAÇÃO CASO A LEGISLAÇÃO NACIONAL AFETE O CUMPRIMENTO DA POLÍTICA

Regra 13A – Os Membros do Grupo comprometem-se a utilizar a presente Política como instrumento de transferência para Entidades Importadoras apenas quando tiverem avaliado em conformidade que a legislação e as práticas do país das Entidades Importadoras (incluindo quaisquer requisitos de divulgação de dados pessoais ou medidas que autorizem o acesso por autoridades públicas) não os impedem de cumprir as respetivas obrigações ao abrigo da presente Política.

Os Membros do Grupo só utilizarão a presente Política como instrumento para salvaguardar as transferências internacionais quando tiverem avaliado que a legislação e as práticas dos países terceiros de destino relevantes, incluindo quaisquer requisitos de divulgação de dados pessoais ou medidas que autorizem o acesso por autoridades públicas, não os impedem de cumprir as respetivas obrigações ao abrigo da presente Política. Tal irá basear-se no entendimento de que a legislação e as práticas que respeitam a essência dos direitos e liberdades fundamentais e não excedem o que é considerado necessário e proporcional numa sociedade democrática não são incompatíveis com a presente Política.

Ao avaliarem a legislação e as práticas dos países terceiros suscetíveis de afetar o cumprimento dos compromissos previstos na presente Política, os Membros do Grupo terão devidamente em conta, em especial, os seguintes elementos:

(i) as circunstâncias específicas da transferência ou do conjunto de transferências, bem como de quaisquer transferências ulteriores previstas para o mesmo ou para outro país terceiro, incluindo:

- as finalidades para as quais são transferidos e tratados os dados (por exemplo, marketing, RH, armazenamento, suporte de TI, etc.);
- os tipos de entidades envolvidas no tratamento (a Entidade Importadora e qualquer destinatário subsequente de uma transferência ulterior);
- o setor económico em que ocorre a transferência ou o conjunto de transferências;
- as categorias e o formato dos dados pessoais transferidos;
- o local onde o tratamento é realizado, incluindo o armazenamento; e
- os canais de transmissão utilizados.

(ii) a legislação e as práticas dos países terceiros de destino relevantes à luz das circunstâncias da transferência. Estas podem incluir: (a) as que exigem a divulgação de dados a autoridades públicas ou autorizam o acesso por parte das mesmas; (b) as que preveem o acesso a estes dados durante o trânsito entre os países das Entidades Exportadoras e os países das Entidades Importadoras; e (c) as limitações e garantias aplicáveis.

(iii) quaisquer garantias contratuais, técnicas ou organizativas relevantes implementadas para complementar as garantias previstas na presente Política. Tal inclui as medidas aplicadas durante a transmissão, bem como as medidas aplicadas ao tratamento dos dados pessoais nos países de destino.

Sempre que seja necessário implementar garantias adicionais às garantias previstas na presente Política, o Membro Responsável pelas RVE e o EPD ou Responsável competente, conforme o caso, serão informados e envolvidos na avaliação. Os Membros do Grupo irão documentar devidamente a referida avaliação, bem como as medidas complementares selecionadas e implementadas. A documentação será disponibilizada à autoridade de controlo competente, mediante pedido.

As Entidades Importadoras irão notificar prontamente as Entidades Exportadoras se, ao utilizarem a presente Política como instrumento de transferência e durante o período em que dela façam parte, tiverem motivos para considerar que estão ou passaram a estar sujeitas a legislação ou práticas que as impeçam de cumprir as respetivas obrigações ao abrigo da presente Política. Tal inclui a impossibilidade de cumprir obrigações após uma alteração da legislação do país terceiro em causa ou a adoção de uma medida (como um pedido de divulgação). Estas informações serão igualmente comunicadas ao Membro Responsável pelas RVE.

Após a verificação da notificação, a Entidade Exportadora competente, juntamente com o Membro Responsável pelas RVE e o EPD ou Responsável competente, conforme o caso, compromete-se a identificar prontamente um conjunto de medidas complementares (por exemplo, medidas técnicas ou organizativas destinadas a assegurar a segurança e a confidencialidade) a adotar pela Entidade Exportadora e/ou Entidade Importadora, a fim de lhes permitir cumprir as respetivas obrigações ao abrigo da presente Política. O mesmo se aplica caso uma Entidade Exportadora tenha motivos para considerar que uma Entidade Importadora deixou de poder cumprir as respetivas obrigações ao abrigo da presente Política.

Sempre que a Entidade Exportadora competente, juntamente com o Membro Responsável pelas RVE e o EPD ou Responsável competente, conforme o caso, avalie que a presente Política (mesmo que seja acompanhada por medidas complementares) não pode ser cumprida relativamente a uma transferência ou um conjunto de transferências, ou quando tal seja determinado pela autoridade de controlo competente, a Entidade

Exportadora competente compromete-se a suspender a transferência ou o conjunto de transferências em causa, bem como todas as transferências relativamente às quais a mesma avaliação e fundamentação conduzam a um resultado semelhante, até que o cumprimento volte a estar assegurado ou a transferência seja cessada.

Na sequência da referida suspensão, a Entidade Exportadora deverá cessar a transferência ou o conjunto de transferências caso a presente Política continue a não poder ser cumprida e o cumprimento não seja restabelecido no prazo de um mês a contar da suspensão. Nesse caso, os dados pessoais transferidos antes da suspensão, bem como quaisquer cópias dos mesmos, serão devolvidos ou destruídos na sua totalidade, mediante escolha da Entidade Exportadora.

O Membro Responsável pelas RVE e o EPD ou Responsável competente, conforme o caso, irão informar todos os restantes Membros do Grupo da avaliação realizada e dos respetivos resultados, para que as medidas complementares identificadas sejam aplicadas caso o mesmo tipo de transferência seja efetuado por qualquer outro Membro do Grupo ou, sempre que não seja possível implementar medidas complementares eficazes, para que as transferências em causa sejam suspensas ou cessadas.

As Entidades Exportadoras irão também acompanhar, de forma contínua e, quando adequado, em colaboração com as Entidades Importadoras, a evolução da situação nos países terceiros para os quais tenham transferido dados pessoais, sempre que essa evolução possa afetar a avaliação inicial do nível de proteção e as decisões adotadas relativamente às transferências.

Regra 13B – As Entidades Importadoras irão assegurar que, caso recebam um pedido juridicamente vinculativo de uma autoridade pública, ao abrigo da legislação do país de destino, para a divulgação de dados pessoais transferidos nos termos da presente Política, ou tomem conhecimento de qualquer acesso direto, por autoridades públicas, a dados pessoais transferidos nos termos da presente Política, em conformidade com a legislação do país de destino, as Entidades Importadoras irão notificar prontamente a Entidade Exportadora e, sempre que possível, o titular dos dados (se necessário, com o apoio da Entidade Exportadora).

As Entidades Importadoras irão notificar prontamente a Entidade Exportadora competente e, sempre que possível, o titular dos dados (se necessário, com o apoio da Entidade Exportadora), caso:

- recebam um pedido juridicamente vinculativo, formulado por uma autoridade pública ao abrigo da legislação do país de destino ou de outro país terceiro, para a divulgação de dados pessoais transferidos nos termos da presente Política (esta notificação incluirá informações sobre os dados pessoais solicitados, a autoridade requerente, o fundamento jurídico do pedido e a resposta facultada); ou

- tomem conhecimento de qualquer acesso direto, por autoridades públicas, a dados pessoais transferidos nos termos da presente Política, em conformidade com a legislação do país de destino (esta notificação incluirá todas as informações de que a Entidade Importadora disponha).

Caso esteja proibida de notificar a Entidade Exportadora e/ou o titular dos dados sobre o acesso, a Entidade Importadora irá envidar os melhores esforços para obter uma dispensa da proibição, a fim de comunicar à Entidade Exportadora o maior número possível de informações, o mais rapidamente possível, e irá documentar os esforços desenvolvidos, por forma a poder demonstrá-los mediante pedido da Entidade Exportadora.

A Entidade Importadora irá fornecer à Entidade Exportadora, em intervalos regulares, o máximo de informações relevantes possível sobre os pedidos recebidos (nomeadamente, o número de pedidos, o tipo de dados solicitados, a autoridade ou as autoridades requerentes, a indicação de os pedidos terem sido ou não impugnados e o resultado da referida impugnação, etc.). Se a Entidade Importadora estiver ou passar a estar

parcial ou totalmente impedida de fornecer à Entidade Exportadora as informações acima referidas, a mesma informará a Entidade Exportadora desse facto sem demora injustificada.

A Entidade Importadora irá conservar as informações acima referidas durante o período em que os dados estiverem sujeitos às garantias previstas na presente Política e disponibilizá-las à autoridade de controlo competente, mediante pedido.

A Entidade Importadora irá analisar a legalidade do pedido de divulgação, em especial se este se mantiver dentro dos poderes conferidos à autoridade pública requerente, e impugnar o pedido se, após uma análise cuidada, concluir que existem motivos razoáveis para considerar que o pedido é ilícito nos termos da legislação do país de destino, das obrigações aplicáveis ao abrigo do direito internacional e dos princípios da comunidade internacional. Nas mesmas condições, a Entidade Importadora irá recorrer, se possível, da decisão. Ao impugnar o pedido, a Entidade Importadora irá procurar obter medidas provisórias destinadas a suspender os efeitos do pedido até que a autoridade judicial competente se pronuncie sobre o seu mérito. A mesma não irá divulgar os dados pessoais solicitados até que tal seja exigido pelas normas processuais aplicáveis.

A Entidade Importadora irá documentar a sua apreciação jurídica e qualquer impugnação do pedido de divulgação e, na medida dos limites permitidos pela legislação do país de destino, irá disponibilizar a documentação à Entidade Exportadora. Da mesma forma, irá disponibilizá-la à autoridade de controlo competente, mediante pedido.

A Entidade Importadora irá fornecer a quantidade mínima de informações permitida ao responder a um pedido de divulgação, com base numa interpretação razoável do mesmo.

Em qualquer caso, os Membros do Grupo irão assegurar que quaisquer transferências de dados pessoais efetuadas ao abrigo da presente Política para uma autoridade pública não são massivas, desproporcionais ou indiscriminadas de forma a exceder o que é considerado necessário numa sociedade democrática.

REGRA 14 – INCUMPRIMENTO DA POLÍTICA E CESSAÇÃO

Regra 14A – As Entidades Exportadoras só irão transferir dados pessoais para as Entidades Importadoras que estiverem efetivamente vinculadas pela presente Política e forem capazes de assegurar o respetivo cumprimento.

Nenhuma transferência será efetuada ao abrigo da presente Política para um Membro do Grupo, salvo se esse Membro do Grupo estiver efetivamente vinculado pela presente Política e for capaz de assegurar o respetivo cumprimento. Sempre que, por qualquer motivo, uma Entidade Importadora não consiga cumprir a presente Política, a mesma informará prontamente a Entidade Exportadora. Caso a Entidade Importadora viole a presente Política ou não seja capaz de a cumprir, a Entidade Exportadora irá suspender ou deixar de efetuar a transferência.

Por decisão da Entidade Exportadora, a Entidade Importadora irá devolver ou eliminar imediata e totalmente os dados pessoais que lhe tiverem sido transferidos ao abrigo da presente Política, quando:

- a Entidade Exportadora tiver suspendido a transferência e o cumprimento da presente Política não for restabelecido num prazo razoável e, em qualquer caso, no prazo de um mês após a suspensão; ou
- a Entidade Importadora violar a presente Política de forma substancial ou persistente; ou
- a Entidade Importadora não cumprir uma decisão vinculativa de um tribunal ou uma autoridade de controlo competente relativa às respetivas obrigações ao abrigo da presente Política.

O mesmo se aplica a quaisquer cópias dos dados. A Entidade Importadora irá certificar a eliminação dos dados perante a Entidade Exportadora. Enquanto os dados não forem eliminados ou devolvidos, a Entidade Importadora continuará a assegurar o cumprimento da presente Política. Quando exista uma proibição legal que impeça a Entidade Importadora de devolver ou eliminar os dados pessoais transferidos, a Entidade Importadora garante que continuará a assegurar o cumprimento da presente Política e que tratará os dados apenas na medida e durante o período legalmente exigidos.

Regra 14B – A Entidade Importadora que deixe de estar vinculada pela presente Política assegura que os dados pessoais são adequadamente conservados, devolvidos ou eliminados, conforme aplicável.

A Entidade Importadora que deixe de estar vinculada pela presente Política poderá conservar, devolver ou eliminar os dados pessoais recebidos ao abrigo da presente Política, conforme aplicável. Se a Entidade Exportadora e a Entidade Importadora acordarem que os dados podem ser conservados pela Entidade Importadora, deverá manter-se a proteção prevista na presente Política.

SECÇÃO C: DIREITOS DOS BENEFICIÁRIOS TERCEIROS

C.1 Os titulares dos dados cujos dados pessoais sejam transferidos para uma Entidade Importadora devem poder beneficiar de determinados direitos na qualidade de beneficiários terceiros. Para o efeito, os titulares dos dados podem exigir o cumprimento das seguintes disposições:

- Regras 1B e 1C da presente Política (relativas à licitude e justiça e ao tratamento de categorias especiais de dados pessoais);
- Regra 2 da presente Política (relativa à transparência e ao tratamento de dados pessoais apenas para uma determinada finalidade);
- Regra 3 da presente Política (relativa à minimização e exatidão dos dados e aos períodos de conservação limitados);
- Regra 4 da presente Política (relativa às medidas de segurança adequadas e às obrigações de notificação de violação de dados);
- Regra 5 da presente Política (relativa ao respeito pelos direitos dos titulares dos dados);
- Regra 6 da presente Política (relativa à proteção adequada das transferências e transferências ulteriores);
- Regra 10 da presente Política (relativa ao tratamento de reclamações);
- Regra 11 da presente Política (relativa à cooperação com as autoridades de controlo competentes);
- Regra 12 da presente Política (relativa à atualização das regras);
- Regra 13 da presente Política (relativa à atuação caso a legislação nacional impeça o cumprimento da Política);
- As disposições constantes das secções C.1 a C.3 que conferem direitos de beneficiários terceiros e estabelecem as regras de responsabilidade e competência jurisdicional ao abrigo da presente Política; e

- O direito de aceder à presente Política disponibilizada na página Web da empresa, na rede interna (acessível aos colaboradores), ou o direito de obter uma cópia em papel da presente Política, bem como uma lista dos Membros do Grupo vinculados pela mesma.

da seguinte forma:

- *apresentando uma reclamação:* os titulares dos dados podem apresentar reclamações junto de um Membro do Grupo (em conformidade com o Procedimento de Tratamento de Reclamações definido no Anexo 2) e da autoridade de controlo do Estado-Membro em que ocorreu a alegada infração ou em que o titular dos dados trabalha ou reside habitualmente; e/ou

- *instaurando ações judiciais:* os titulares dos dados podem instaurar ações judiciais contra os Membros do Grupo nos tribunais de um Estado-Membro em que o Membro do Grupo tem um estabelecimento ou no Estado-Membro em que o titular dos dados tem residência habitual.

Conforme previsto nas secções C.2 a C.4, sempre que uma infração for cometida por um Membro do Grupo localizado fora do EEE, os titulares dos dados irão conservar o direito de apresentar reclamações e instaurar ações judiciais contra o Membro Responsável pelas RVE designado, como se a infração tivesse sido cometida por essa entidade no Estado-Membro em que a mesma está estabelecida.

Estes direitos não se estendem aos elementos da presente Política relativos aos mecanismos internos implementados pelos Membros do Grupo, tais como os detalhes da formação, o programa de auditoria, a rede de conformidade e o mecanismo de atualização da presente Política.

Além disso, os Membros do Grupo aceitam que os titulares dos dados podem ser representados por um organismo, organização ou associação sem fins lucrativos, nas condições previstas no artigo 80.º, n.º 1, do RGPD.

C.2 Os titulares dos dados podem também obter a reparação adequada junto do Membro Responsável pelas RVE, que aceita tomar as medidas necessárias para sanar qualquer violação das disposições previstas na secção C.1 por parte das Entidades Importadoras e, quando aplicável, obter junto do Membro Responsável pelas RVE uma indemnização por eventuais danos (patrimoniais ou não patrimoniais) sofridos na sequência da violação de qualquer uma das disposições previstas na secção C.1 por uma Entidade Importadora, em conformidade com a decisão de um tribunal ou outra autoridade competente.

C.3 Para que não subsistam dúvidas, os titulares dos dados irão beneficiar dos direitos de beneficiários terceiros descritos na presente Secção C, e os tribunais europeus ou as autoridades de controlo competentes terão competência como se a violação das disposições descritas na presente Secção C, ou de qualquer uma delas, tivesse sido cometida pelo Membro Responsável pelas RVE.

C.4 Sempre que for apresentada uma ação em que um titular dos dados tenha sofrido danos na sequência da violação da presente Política, os Membros do Grupo acordam que o ónus da prova de demonstrar que uma Entidade Importadora não é responsável pela violação, ou que tal violação não ocorreu, cairá sobre o Membro Responsável pelas RVE.

PARTE III: ANEXOS

ANEXO 1

PROGRAMA DE AUDITORIA

1. INTRODUÇÃO

1.1 Os Membros do Grupo são obrigados a auditar a respetiva conformidade com a presente Política, devendo para isso cumprir determinadas condições. O presente documento descreve a forma como os Membros do Grupo dão cumprimento a estes requisitos.

1.2 As atividades correntes dos EPD e dos Responsáveis incluem a prestação de orientação sobre o tratamento de dados pessoais sujeito à presente Política e a avaliação do tratamento de dados pessoais efetuado pelos Membros do Grupo quanto a potenciais riscos relacionados com a privacidade no âmbito da atividade quotidiana. Por conseguinte, o tratamento de dados pessoais está sujeito a uma revisão e avaliação pormenorizada e contínua.

1.3 Enquanto 2LoD Global, o Gabinete Corporativo de Proteção de Dados assume as funções de monitorização e controlo, incluindo a supervisão da conformidade do Grupo Santander em matéria de proteção de dados.

1.4 Por outro lado, o Programa de Auditoria consiste na avaliação formal e independente realizada pela terceira linha de defesa (3LoD), a fim de assegurar o cumprimento da presente Política, conforme exigido pelas autoridades de controlo competentes. O parecer emitido pela Auditoria (3LoD) é independente e não substitui as responsabilidades de controlo e supervisão da 1LoD e 2LoD, as quais farão também parte do âmbito da auditoria durante a avaliação do grau de integração e implementação da presente Política.

2. ABORDAGEM

2.1 <u>Visão geral da auditoria</u>

A entidade responsável pela realização das auditorias de conformidade com a presente Política e por assegurar que as referidas auditorias abrangem todos os aspetos da Política pode variar em função das circunstâncias específicas de cada Membro do Grupo. Normalmente, as auditorias são supervisionadas por auditores internos ou externos acreditados, conforme aplicável (que garantiram independência no desempenho das suas funções relacionadas com as auditorias). O auditor competente será responsável por assegurar que quaisquer problemas ou casos de incumprimento são levados ao conhecimento da direção de topo e que quaisquer medidas corretivas destinadas a assegurar a conformidade são devidamente implementadas num prazo razoável.

2.2 <u>Calendarização e âmbito da auditoria</u>

2.2.1 O departamento de Auditoria Interna irá determinar, de acordo com a respetiva metodologia de avaliação de riscos, a calendarização das auditorias, no âmbito de um ciclo de auditoria máximo de 4 anos.

Não obstante, as primeiras auditorias terão lugar nos primeiros 24 meses após a aprovação formal da presente Política e a sua consequente entrada em vigor. Posteriormente, a auditoria será realizada de acordo com a metodologia de auditoria baseada em riscos aplicável, conforme indicado no primeiro parágrafo da presente secção 2.2.

Em todos os casos, os Membros do Grupo serão obrigados a realizar uma auditoria quando: (i) existirem indícios de incumprimento da presente Política; ou (ii) a Equipa de Privacidade solicitar uma auditoria específica *(ad hoc)*.

2.2.2 Do mesmo modo, o âmbito e a cobertura da auditoria serão determinados pelo departamento de Auditoria Interna com base numa análise baseada em riscos realizada em função da metodologia aprovada.

2.2.3 Todos os aspetos da presente Política (por exemplo, aplicações, sistemas de TI, transferências ulteriores, etc.), incluindo os métodos e planos de ação destinados a assegurar a implementação das medidas corretivas, serão objeto de revisão segundo uma abordagem baseada em riscos para determinar o âmbito específico da auditoria, sendo os mesmos revistos, conforme descrito acima, em intervalos regulares adequados.

2.3 Auditores

2.3.1 As auditorias previstas no presente documento serão realizadas por auditores internos do departamento de Auditoria Interna ou por auditores externos acreditados, conforme aplicável. Sempre que as auditorias forem realizadas por auditores externos, deverão estar reunidas as seguintes condições:

(a) Realizar uma diligência prévia adequada antes da sua seleção, a fim de assegurar que os auditores em causa possuem as qualificações e o estatuto adequados para prestar assistência no âmbito deste exercício; e

(b) Celebrar um contrato com os referidos auditores para regular a prestação dos seus serviços em conformidade com a regulamentação aplicável.

2.4 Independência

2.4.1 As pessoas responsáveis por decidir sobre o programa de auditoria ou por realizar as auditorias têm a respetiva independência garantida com vista ao desempenho das suas funções.

2.5 Relatório

2.5.1 Após a conclusão da auditoria e consoante a natureza da mesma, o relatório e as respetivas conclusões serão disponibilizados à direção de topo, ao Gabinete Corporativo de Proteção de Dados, ao EPD ou Responsável competente, sendo igualmente comunicados ao Comité de Auditoria do Conselho de Administração e ao Conselho de Administração do Membro Responsável pelas RVE. O relatório de auditoria incluirá também informações sobre quaisquer medidas corretivas necessárias, bem como recomendações e prazos para a implementação dessas medidas.

2.5.2 Os Membros do Grupo acordam em disponibilizar cópias dos resultados de qualquer auditoria à presente Política a qualquer autoridade de controlo competente, mediante pedido.

2.5.3 O EPD ou Responsável competente será responsável por estabelecer a ligação com as autoridades de controlo competentes para efeitos da prestação das informações acima referidas.

ANEXO 2

PROCEDIMENTO DE TRATAMENTO DE RECLAMAÇÕES

1. INTRODUÇÃO

1.1 O objetivo do presente Procedimento de Tratamento de Reclamações consiste em explicar a forma como serão tratadas as reclamações apresentadas por um titular dos dados cujos dados pessoais sejam tratados pelos Membros do Grupo ao abrigo da presente Política.

2. COMO OS TITULARES DOS DADOS PODEM APRESENTAR RECLAMAÇÕES

Todas as reclamações dos titulares dos dados cujos dados pessoais sejam tratados em conformidade com a presente Política podem ser apresentadas, por escrito (incluindo por e-mail), ao EPD ou Responsável competente, conforme o caso. Os titulares dos dados podem apresentar uma reclamação utilizando os seguintes contactos:

Atenção: Equipa de Privacidade

Morada: [inserir morada postal]

E-mail: uma lista dos endereços de e-mail relevantes é apresentada aqui.

Em qualquer caso, se as reclamações forem apresentadas por qualquer outro meio, serão igualmente tratadas, desde que sejam devidamente comunicadas ao Membro do Grupo competente.

3. QUEM TRATA DAS RECLAMAÇÕES?

3.1 O EPD ou Responsável competente, conforme o caso, tratará todas as reclamações apresentadas ao abrigo da presente Política relativas ao tratamento de dados pessoais. O EPD ou Responsável, conforme o caso, irá articular-se com as unidades de negócio relevantes para investigar a reclamação e irá coordenar uma resposta (que incluirá informações dirigidas ao autor da reclamação sobre as medidas adotadas).

3.2 Qual é o prazo de resposta?

O EPD ou Responsável competente, com o apoio da Equipa de Privacidade, irá acusar a receção da reclamação ao titular dos dados em causa no prazo de dez dias úteis, procedendo posteriormente à sua investigação e apresentando uma resposta de mérito, mediante a prestação de informações sobre as medidas adotadas, sem demora injustificada e, em qualquer caso, no prazo de um mês civil. Se, devido à complexidade da reclamação ou ao número de pedidos, não for possível apresentar uma resposta de mérito dentro do prazo, o EPD ou Responsável competente, com o apoio da Equipa de Privacidade, irá informar o autor da reclamação, no prazo de um mês civil a contar da receção da reclamação, das razões do atraso e irá fornecer uma estimativa razoável do prazo de resposta (não superior a mais dois meses civis a contar da data em que o titular dos dados é informado da prorrogação).

Se o prazo de resposta não for cumprido e a resposta à reclamação sofrer atrasos sem que tenha sido apresentada qualquer justificação, o titular dos dados poderá comunicar esse facto ao EPD ou Responsável que, sem demora injustificada e, em qualquer caso, no prazo de dez dias civis, irá explicar as razões do atraso e informar o titular dos dados sobre as medidas adotadas até ao momento. O

assunto será remetido ao Gabinete Corporativo de Proteção de Dados (juntamente com um relatório fundamentado que determine as medidas a adotar), que irá analisar o caso e aconselhar o EPD ou Responsável sobre a forma de resolver o objeto da reclamação o mais rapidamente possível. Em qualquer caso, o titular dos dados também pode exercer os direitos descritos na secção 3.4 do presente Anexo 2.

3.3 Quando o autor da reclamação contesta uma conclusão ou o indeferimento de uma reclamação

Se uma reclamação for considerada procedente, o EPD ou Responsável irá adotar as medidas necessárias para resolver a questão suscitada pelo titular dos dados e irá informá-lo em conformidade.

Se o autor da reclamação contestar a resposta do EPD ou Responsável (incluindo quando essa resposta consiste no indeferimento da reclamação ou na recusa de lhe dar seguimento) ou qualquer aspeto das conclusões, poderá comunicar esse facto ao EPD ou Responsável competente. O assunto será remetido ao Gabinete Corporativo de Proteção de Dados, que irá analisar o caso e, através do EPD ou Responsável da entidade, irá comunicar ao autor da reclamação a decisão final, aceitando a conclusão inicial ou apresentando uma conclusão nova. O Gabinete Local de Proteção de Dados irá responder ao autor da reclamação no prazo de um mês civil a contar da remessa do processo. Se, devido à complexidade da reclamação, não for possível apresentar uma resposta de mérito dentro do prazo, o Gabinete Corporativo de Proteção de Dados irá informar o autor da reclamação, no prazo de um mês civil a contar da receção da remessa, das razões do atraso e irá fornecer uma estimativa razoável do prazo de resposta (não superior a mais dois meses civis). Se a reclamação for julgada procedente, o Gabinete Corporativo de Proteção de Dados irá providenciar a adoção das medidas necessárias na sequência da decisão.

3.4 Mecanismos de reclamação alternativos

Os titulares dos dados cujos dados pessoais são tratados em conformidade com a presente Política também têm o direito de: (i) apresentar uma reclamação à autoridade de controlo do Estado-Membro em que ocorreu a alegada infração, ou em que o titular dos dados trabalha ou reside habitualmente; e/ou (ii) instaurar uma ação junto de um tribunal competente do país europeu em que o Membro do Grupo está estabelecido ou do país europeu em que o titular dos dados reside. Conforme previsto nas secções C.2 a C.4, sempre que uma infração for cometida por um Membro do Grupo localizado fora do EEE, os titulares dos dados irão conservar o direito de apresentar reclamações e instaurar ações judiciais contra o Membro Responsável pelas RVE designado, como se a infração tivesse sido cometida por essa entidade no Estado-Membro em que a mesma está estabelecida. Estes direitos aplicam-se independentemente de os titulares dos dados terem ou não apresentado previamente uma reclamação a um Membro do Grupo através do presente Procedimento de Tratamento de Reclamações.

ANEXO 3

PROCEDIMENTO DE COOPERAÇÃO

1. PROCEDIMENTO DE COOPERAÇÃO

1.1 O presente Procedimento de Cooperação define a forma como os Membros do Grupo irão cooperar com as autoridades de controlo competentes e aceitar ser objeto de auditorias e inspeções das mesmas (incluindo no local, quando necessário) no âmbito da presente Política, além de ter em consideração os respetivos pareceres e respeitar as decisões apresentadas sobre eventuais questões relacionadas com a presente Política.

1.2 Sempre que necessário, os Membros do Grupo irão disponibilizar o pessoal adequado para dialogar com a autoridade de controlo competente relativamente à presente Política.

1.3 Mediante pedido, o EPD, o Responsável ou o departamento de Auditoria Interna competente, conforme aplicável, irá fornecer à autoridade de controlo competente cópias dos resultados de qualquer auditoria realizada à presente Política, nos termos do Anexo 1, bem como quaisquer informações relativas às operações de tratamento abrangidas pela presente Política, recordando à autoridade de controlo, no momento da disponibilização das informações, o seu dever de sigilo profissional.

1.4 Os Membros do Grupo aceitam que as autoridades de controlo competentes realizem auditorias ou inspeções de proteção de dados (incluindo no local, quando necessário), em conformidade com a Legislação Europeia em matéria de Proteção de Dados aplicável à Entidade Exportadora relevante.

1.5 Todos os Membros do Grupo aceitam ser auditados pelas autoridades de controlo competentes, em conformidade com os procedimentos de auditoria aplicáveis das referidas autoridades.

1.6 Os Membros do Grupo aceitam que qualquer litígio relacionado com o exercício dos poderes de supervisão das autoridades de controlo competentes no âmbito da presente Política seja resolvido pelos tribunais do Estado-Membro em que a autoridade de controlo em causa se encontra estabelecida, em conformidade com a legislação processual do Estado-Membro.

ANEXO 4

PROCEDIMENTO DE ATUALIZAÇÃO

1. INTRODUÇÃO E PRINCÍPIOS GERAIS

1.1 O presente Procedimento de Atualização define a forma como serão comunicadas as alterações à Política junto das autoridades de controlo competentes, dos titulares dos dados e dos Membros do Grupo vinculados pela Política.

1.2 A Política será mantida atualizada, de modo a refletir a situação e o enquadramento vigentes em matéria de proteção de dados pessoais.

2. ALTERAÇÕES MATERIAIS À POLÍTICA

2.1 O EPD do Banco Santander e o Departamento Jurídico Corporativo irão comunicar antecipadamente à Agência Espanhola de Proteção de Dados (o «**Coordenador das RVE**») e, através do Coordenador das RVE, às autoridades de controlo, quaisquer alterações materiais à Política (isto é, quaisquer alterações suscetíveis de prejudicar o nível de proteção assegurado pela Política ou afetar significativamente a Política, por exemplo, alterações ao carácter vinculativo da mesma). Esta comunicação irá incluir uma breve explicação das razões subjacentes à atualização. A autoridade de controlo competente irá também avaliar se as alterações efetuadas exigem uma nova aprovação.

3. OUTRAS ALTERAÇÕES À POLÍTICA

3.1 O EPD do Banco Santander e o Departamento Jurídico Corporativo irão comunicar ao Coordenador das RVE (e, através deste, às restantes autoridades de controlo competentes), quando solicitado e, pelo menos, uma vez por ano, as alterações introduzidas na Política (ou a inexistência das mesmas). Esta atualização anual irá também renovar a confirmação de que o Membro Responsável pelas RVE dispõe de ativos suficientes ou adotou mecanismos adequados que lhe permitem pagar indemnizações por danos resultantes de uma violação da Política.

3.2 Alguns exemplos das alterações acima referidas podem incluir alterações de natureza administrativa (incluindo atualizações da lista de Membros do Grupo); alterações decorrentes de modificações da Legislação Europeia em matéria de Proteção de Dados aplicável; ou alterações resultantes de medidas, orientações ou decisões legislativas, judiciais ou das autoridades de controlo (incluindo orientações do Comité Europeu para a Proteção de Dados). O Banco Santander irá também fornecer ao Coordenador das RVE e às restantes autoridades de controlo uma breve explicação das razões subjacentes a quaisquer alterações comunicadas à Política.

4. NOVOS MEMBROS DO GRUPO

4.1 Os EPD e os Responsáveis (em conjunto com a Equipa de Privacidade) irão assegurar que todos os novos Membros do Grupo ficam efetivamente vinculados pela Política e são capazes de a cumprir antes de efetuarem qualquer transferência de dados pessoais para os Membros do Grupo.

5. COMUNICAÇÃO E REGISTO DE ALTERAÇÕES À POLÍTICA

5.1 A Política inclui um registo de alterações, que indica a data das revisões da Política e os detalhes das alterações efetuadas. O Departamento Jurídico Corporativo irá manter uma lista atualizada das alterações introduzidas na Política e o Gabinete Corporativo de Proteção de Dados irá manter a lista dos Membros do Grupo vinculados pela mesma.

5.2 O Departamento Jurídico Corporativo, com o apoio do Gabinete Corporativo de Proteção de Dados, irá comunicar todas as alterações à Política, sejam elas materiais ou de outra natureza:

(a) aos Membros do Grupo vinculados pela Política, sem demora injustificada, e irá publicar uma versão atualizada da presente Política na rede interna do Grupo Santander;

(b) de forma sistemática, aos titulares dos dados que beneficiarem da presente Política, através do sítio Web da empresa (Web Corporativa Santander); e

(c) mediante pedido e através dos EPD locais competentes (ou figura local equivalente), à autoridade de controlo competente.