GRUPO SANTANDER

NORMAS CORPORATIVAS VINCULANTES – POLÍTICA DE RESPONSABLE DEL TRATAMIENTO

CONTENIDO PÁGINA

INTRODUCCIÓN

Las presentes Normas Corporativas Vinculantes - Política de Responsable del Tratamiento (en adelante, "**BCR**" por sus siglas en inglés) y sus Apéndices (conjuntamente, la "**Política**") establecen el enfoque adoptado por Banco Santander, S.A. ("**Banco Santander**") con respecto a la protección y gestión de los datos personales por parte de los miembros del Grupo Santander -según se define más adelante- adheridos a esta Política en el contexto de las transferencias internacionales de dichos datos entre Miembros del Grupo -según se define más adelante-.

Banco Santander es la sociedad matriz y sede de uno de los mayores grupos financieros de España compuesto por filiales tanto españolas como extranjeras ("**Grupo Santander**") dedicado a la prestación de servicios financieros globales en todo el mundo a través de las siguientes áreas principalmente: (i) ***Retail & Commercial Banking***: que engloba todas las operaciones de banca minorista y comercial de Grupo Santander; (ii) ***Corporate & Investment Banking***: que da soporte a clientes corporativos e institucionales ofreciendo soluciones personalizadas y productos mayoristas de alto valor añadido a través de las divisiones *Markets, Investment Banking (Global Debt Finance y Corporate Finance)* y *Global Transactional Banking*; (iii) ***Wealth Management & Insurance*:** que integra los negocios de banca privada, gestión de activos y seguros a través *de Santander Private Banking, Santander Asset Management* y *Santander Insurance*; (iv) ***Digital Consumer Bank***: que combina la plataforma digital Openbank y *Santander Consumer Finance,* creando un modelo único en todos los mercados para los consumidores y el negocio de financiación de automóviles; y (v) ***PagoNxt & Cards***: que engloba PagoNxt, que agluitina todos los negocios de pagos de Grupo Santander, y *Global Cards*, la plataforma y el negocio de tarjetas de Grupo Santander, que ofrece opciones digitales de pago y soluciones tecnológicas globales para los bancos y nuevos clientes de Grupo Santander. Además de lo anterior, Grupo Santander también está formado por la **Sede Corporativa y otros departamentos al servicio de todo el Grupo**: que son las áreas encargadas de dar soporte y asistir a todos los Miembros del Grupo en todas las acciones necesarias a nivel de grupo no estrictamente relacionadas con su actividad principal (*e.g.*, gestión de empleados, cumplimiento normativo, auditorías, gestión de riesgos, etc.).

Además de otras definiciones previstas en la presente Política, aplicarán los siguientes términos:

"**Ley Local de PD Aplicable"** significa cualquier ley nacional / local de protección de datos (incluida, en su caso, la Normativa Europea de Protección de Datos) aplicable a los Miembros del Grupo, en la medida en que respeten la esencia de los derechos y libertades fundamentales y no excedan de lo necesario y proporcionado en una sociedad democrática conforme a lo exigido en la Regla 13 de esta Política.

"**autoridad de control competente"** significa la autoridad de control del EEE competente respecto de la Entidad Exportadora;

"**responsable del tratamiento**" significa una persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales;

"**Europa"** o "**EEE**" se refiere a los países del Espacio Económico Europeo;

"**Normativa Europea de Protección de Datos"** significa el RGPD y cualquier ley de protección de datos de un Estado miembro de Europa, incluida la legislación local que implementa los requisitos del RGPD, como la normativa de desarrollo, en cada caso según se vaya modificando;

"**Entidad Exportadora"** significa un Miembro del Grupo establecido en Europa, o sujeto a la Normativa Europea de Protección de Datos, que transfiere, o pone a disposición, datos personales a una Entidad Importadora en virtud de la presente Política;

"RGPD" significa el Reglamento 2016/679 de la Unión Europea (UE) (el Reglamento General de Protección de Datos);

"**Miembro del Grupo**" significa los miembros del Grupo Santander adheridos a esta Política;

"**Entidad Importadora**" significa un Miembro del Grupo establecido fuera de Europa y que recibe datos personales de una Entidad Exportadora y trata los datos personales transferidos fuera del EEE;

"Miembro Responsable de las BCR" significa Banco Santander (i.e. Banco Santander, S.A., tal y como se define a continuación);

"**datos personales**" significa toda información sobre una persona física identificada o identificable. Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como e.g. un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

"**tratamiento"** significa cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

"**encargado del tratamiento**" significa una persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

"**elaboración de perfiles"** significa cualquier forma de tratamiento automatizado de datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o movimientos de dicha persona física;

"**categorías especiales de datos personales**" o "**datos sensibles"** significa los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física; y

"**autoridad de control"**: una autoridad pública independiente establecida en una jurisdicción europea por un Estado Miembro, que es responsable de supervisar la aplicación de la Normativa Europea de Protección de Datos con el fin de proteger los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento y de facilitar la libre circulación de datos personales dentro del EEE.

La presente Política se aplica a todos los datos personales sujetos a la Normativa Europea de Protección de Datos que se transfieren de Entidades Exportadoras a Entidades Importadoras y a las transferencias ulteriores de Entidades Importadoras a otras Entidades Importadoras o a terceros fuera del EEE (de conformidad con los requisitos establecidos en la Regla 6 a continuación). Por lo tanto, todas las obligaciones y requisitos impuestos

a los Miembros del Grupo en virtud de la presente Política serán aplicables en la medida en que se refieran a datos personales que se encuentren bajo ese ámbito de aplicación.

Esta Política se aplica a todos los datos personales tratados por los Miembros del Grupo, tal y como se describe en las secciones "*¿Qué datos personales cubre esta Política?*" y "*¿Con qué fines se transfieren datos personales en virtud de esta Política?*".

Los Miembros del Grupo y sus empleados deben cumplir y respetar plenamente la presente Política en el curso del tratamiento de datos personales bajo la misma.

Esta Política es adicional a, y no sustituye o reemplaza, cualquier requisito o norma específica en materia de confidencialidad o deber de secreto que pueda resultar de aplicación a un área de negocio o departamento dentro del Grupo Santander o según lo exija la legislación aplicable (siempre que dicha legislación cumpla con los requisitos establecidos en la Regla 13 de la presente Política).

Esta Política, junto con una lista de los Miembros del Grupo actuales y sus datos de contacto, tal y como se incluye en el Apéndice 5, se publica en la página web de la empresa, accesible públicamente aquí.

Aplicación a transferencias realizadas por Miembros del Grupo no sujetos a la Normativa Europea de Protección de Datos

Si un Miembro del Grupo no sujeto a la Normativa Europea de Protección de Datos también tiene restricciones aplicables a transferencias internacionales de datos personales en virtud de su Ley Local de PD Aplicable y las autoridades locales de dichos países reconocen esta Política (en su totalidad o en parte, según lo exija la Ley Local de PD Aplicable) como un mecanismo válido para legitimar las transferencias internacionales de datos personales , esta Política también podrá aplicarse a los datos personales transferidos desde dichos países a las Entidades Importadoras. A efectos aclaratorios, esto se entenderá sin perjuicio de la aplicación al Miembro del Grupo fuera de Europa de su Ley Local de PD Aplicable.

En estos casos, las definiciones anteriores deben interpretarse en el sentido de que el Miembro del Grupo que transfiere datos personales no sujeto a la Normativa Europea de Protección de Datos es la Entidad Exportadora. En consecuencia, la Política deberá interpretarse y aplicarse *mutatis mutandis* (*e.g.,* la Normativa Europea de Protección de Datos se interpretará como la Ley Local de PD Aplicable, la autoridad de control competente como la autoridad local competente en la jurisdicción pertinente o el Estado Miembro como el país en cuestión).

En este contexto, el Miembro del Grupo que transfiera datos personales no sujetos a la Normativa Europea de Protección de Datos actuará como Miembro Responsable de las BCR en relación con dicha(s) transferencia(s) internacional(es) de datos.

PARTE I: ANTECEDENTES Y ACCIONES

¿QUÉ ES LA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS?

La Normativa Europea de Protección de Datos otorga a las personas el derecho a controlar cómo se tratan sus datos personales. Según la Normativa Europea de Protección de Datos, cuando una organización trata datos personales para sus propios fines, se considera que esa organización es responsable del tratamiento de esa información y, por tanto, es la principal responsable de cumplir los requisitos legales. Por ejemplo, cuando somos un empleador, somos los responsables del tratamiento de los datos personales que tratamos sobre nuestros empleados.

Cuando, por el contrario, una organización trata información por cuenta de otra entidad (e.g., para prestar un servicio), la primera se considera encargada del tratamiento.

¿CÓMO AFECTA LA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS A LAS TRANSFERENCIAS DE DATOS PERSONALES ENTRE MIEMBROS DEL GRUPO?

La Normativa Europea de Protección de Datos no permite la transferencia de datos personales a países, territorios u organizaciones internacionales fuera de Europa que no garanticen un nivel de protección adecuado de los derechos de protección de datos de las personas. Dado que la Comisión Europea considera que algunos de los países en los que operan los Miembros del Grupo no garantizan un nivel de protección adecuado, deben establecerse garantías adecuadas para cumplir los requisitos de la Normativa Europea de Protección de Datos.

¿QUÉ HACEN LOS MIEMBROS DEL GRUPO AL RESPECTO?

Los Miembros del Grupo deben tomar medidas adecuadas para garantizar que el tratamiento de los datos personales que transfieren internacionalmente es seguro y lícito. El objetivo de esta Política es, por lo tanto, establecer un marco para satisfacer las normas contenidas en la Normativa Europea de Protección de Datos y, como resultado, proporcionar un nivel de protección adecuado para todos los datos personales que se transfieren de Entidades Exportadoras a Entidades Importadoras.

Esta Política es jurídicamente vinculante y se aplica a todos los Miembros del Grupo y a sus empleados cuando dichos Miembros del Grupo tratan datos personales tanto manualmente como por medios automatizados. Exige que los Miembros del Grupo cumplan las Reglas establecidas en la Parte II de esta Política (según proceda) junto con las políticas y procedimientos establecidos en los Apéndices de la Parte III de esta Política. Si una Entidad Importadora está sujeta a una Ley Local de PD Aplicable reconocida por proporcionar un nivel de protección adecuado en virtud de la Ley Local de PD Aplicable de la Entidad Exportadora y ofrece un nivel de protección equivalente al descrito en esta Política, se considerarán válidos los procesos y procedimientos locales que cumplan sustancialmente los requisitos de esta Política, aunque introduzcan diferencias o variaciones procedimentales (e.g., equipos locales encargados de determinados procedimientos), siempre que dichas variaciones sean coherentes con esta Política. Las transferencias internacionales cubiertas por esta Política incluyen las transferencias de datos personales desde los Miembros del Grupo cubiertos por el ámbito territorial del RGPD conforme al artículo 3 RGPD a Miembros del Grupo situados fuera del EEE, así como transferencias ulteriores a otros Miembros del Grupo o a terceros externos (de conformidad con los requisitos establecidos en la Regla 6 a continuación) fuera del EEE.

¿QUÉ OCURRE CON LOS MIEMBROS DEL GRUPO NO SUJETOS A LA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS QUE EXPORTAN DATOS?

Como se explica en la introducción, y con el fin de diseñar un paraguas global de protección de datos para el Grupo Santander, si un Miembro del Grupo no sujeto a la Normativa Europea de Protección de Datos también tiene restricciones aplicables a transferencias internacionales de datos personales en virtud de su Ley Local de DP Aplicable y las autoridades locales de dichos países reconocen esta Política (en su totalidad o en parte, según lo exija la Ley Local de DP Aplicable) como un mecanismo válido para legitimar las transferencias internacionales de datos personales, esta Política también podrá aplicarse a los datos personales transferidos desde dichos países a las Entidades Importadoras. A efectos aclaratorios, esto se entenderá sin perjuicio de la aplicación al Miembro del Grupo fuera de Europa de su Ley Local de PD Aplicable.

¿QUÉ DATOS PERSONALES CUBRE ESTA POLÍTICA?

Los datos personales tratados en virtud de esta Política incluyen:

- En relación con los datos personales de **empleados actuales y pasados y otros miembros del personal (como becarios, *secondees* o autónomos):**

  (a) Datos personales y de contacto (*e.g.,* nombre, segundo nombre, apellidos, título, alias, firma, sexo, fecha de nacimiento, nacionalidad, números / documentos nacionales de identidad, dirección de correo electrónico, dirección postal, números de teléfono, fotografía, permisos de trabajo, etc.); **(b) Datos de empleo, incluyendo historial laboral, condiciones de trabajo y datos de contacto** (*e.g.,* correo electrónico y número de teléfono de la empresa, número de identificación del empleado, nombre de usuario / asignación de clave (*i.e.,* utilizada para el acceso al terminal de trabajo), historial laboral, puesto actual, función, tareas, empresa, centro de negocio, unidad de negocio, número de identificación del departamento, número de identificación de la sucursal, país de actividad, identificación y nombre del supervisor o supervisores, identificación y nombre del subordinado o subordinados, situación y tipo de empleo, si el empleado es externo, fecha de contratación, fecha de inicio del puesto, (si procede) fecha de terminación, datos contractuales, planes de jubilación, flexibilidad laboral, solicitudes de traslados, dotación, datos de cumplimiento de políticas internas u otras legalmente aplicables, evaluaciones y valoraciones del rendimiento (incluidas las opiniones de responsables, partes interesadas y otras personas que trabajen con el empleado), ascensos y expedientes disciplinarios, etc.); **(c) Datos de talento, solicitudes de candidatura y contratación, educación y formación** (*e.g.,* datos contenidos en cartas de presentación y currículum o CV, datos sobre el plan de desarrollo y evaluación, datos de formación, página web personal o perfil de LinkedIn proporcionados directamente por los empleados, antecedentes y referencias de empleos anteriores, historial educativo, cualificaciones profesionales, idiomas y otras habilidades relevantes, etc.); **(d) Información financiera, incluidas nóminas y remuneraciones** (*e.g.*, datos de la cuenta bancaria, salario, planes de beneficios, bonus, divisa, retribución variable, datos sobre opciones sobre acciones, concesiones de acciones y otros premios, frecuencia de pago, fecha efectiva de la remuneración actual, revisiones salariales, identificación y código fiscal, etc.); **(e) Datos de seguridad y tecnologías de la información (IT)** (*e.g.* identificación de usuario, clave de acceso a herramientas, inicios de sesión, credenciales y perfiles de seguridad, correos electrónicos transmitidos desde y recibidos en las cuentas de correo electrónico de la empresa (en la medida en que esté legalmente permitido), información captada a través del uso de IT, incluida la información de acceso y autenticación, historial de navegación por Internet, números de teléfono marcados, documentos y archivos almacenados en los sistemas o redes de la empresa (incluidos los escritorios de los ordenadores), registros / *logs*, dirección IP, intentos de inicio de sesión con éxito y fallidos, información recabada a través de *cookies* u otras tecnologías de seguimiento similares, etc.); **(f) Datos sobre el horario de trabajo** (*e.g.*, vacaciones, días y tiempo libre, otras bajas y justificantes (si procede), fechas de reincorporación tras las bajas, otros datos sobre ausencias, registro de horas

trabajadas (cuando la ley lo exija / permita), horas extraordinarias, turnos de trabajo, etc.); y **(g) Cualquier otra información facilitada voluntariamente por los interesados** (*e.g.*, a través de encuestas de satisfacción u otras encuestas, etc.).

Asimismo, los Miembros del Grupo podrán tratar **categorías especiales de datos personales** (**en particular, aunque no exclusivamente, datos de salud y afiliación sindical**) cuando sea necesario y lo exija o permita la legislación aplicable para los fines descritos en el apartado siguiente.

- En relación con los datos personales de **familiares de empleados**:

  (a) Datos personales y de contacto (*e.g.,* nombre, apellidos, sexo, números / documentos nacionales de identidad, datos de contacto como el número de contacto en caso de emergencia, etc.); y **(b) Otra información sobre los empleados en relación o sobre su familia cuando sea legalmente necesario / permitido** (*e.g.,* grupo familiar y situación, relación con el empleado, nombre y otra información relevante sobre los hijos y otras personas a cargo, estado civil, datos de cumplimiento de políticas internas u otras legalmente aplicables, etc.).

- En relación con los datos personales **de candidatos actuales y pasados**:

  (a) Datos personales y de contacto (*e.g.,* nombre, apellidos, país, estado y ciudad de residencia, dirección de correo electrónico, dirección postal, números de teléfono, nacionalidad, etc.); **(b) Datos de contratación, educación y formación** (*e.g.,* datos contenidos en las cartas de presentación y el currículum / CV, página web personal o perfil de LinkedIn facilitados directamente por los candidatos, antecedentes laborales y referencias, historial educativo, cualificaciones profesionales, idiomas y otras competencias pertinentes, datos sobre las calificaciones de la gestión del rendimiento, plan de desarrollo y disposición a trasladarse, datos personales derivados de la participación de los candidatos en el proceso de contratación como por ejemplo los obtenidos durante las entrevistas personales y los correos electrónicos intercambiados con respecto a las solicitudes o las conversaciones, etc.); y **(c) Información de voz e imagen** (*e.g.,* la voz y la imagen captadas en fotografías, grabaciones de vídeo o audio en el contexto de entrevistas realizadas por teléfono o videoconferencia, etc.).

- En relación con los datos personales de **clientes y consumidores potenciales y actuales** (incluidos los de sus empleados, representantes y/o agentes, según proceda, usuarios autorizados y usuarios de la página web):

  (a) Datos personales y de contacto (*e.g.,* nombre, segundo nombre, apellidos, número de teléfono, dirección de correo electrónico, dirección postal, país de residencia, región, ciudadanía o nacionalidad, números / documentos nacionales de identidad, sexo, idioma, fecha de nacimiento, país de nacimiento, estado civil, datos sobre circunstancias familiares o sociales (*e.g.,* número de personas a cargo), si la persona es menor de edad o necesita un representante legal, datos demográficos y socioeconómicos, etc.); **(b) Datos profesionales** (*e.g.,* profesión, cargo, historial laboral y educativo, datos de la empresa, datos de contacto profesionales, puesto, categoría del puesto, título del puesto, etc.); **(c) Datos (pre)contractuales** (*e.g.,* código de categoría, capacidad jurídica, datos relacionados con poderes de representación, tipo, número de registro e indicador interno de cliente, nivel de vinculación, relación comercial con Santander, productos o servicios contratados o solicitados, *scoring* de riesgo, información de agencias de crédito, órdenes de compra, datos estadísticos, facturas, información sobre bienes y activos, subvenciones, información sobre cuentas y operaciones, en la medida en que lo permita la legislación aplicable, contratos y otros acuerdos que puedan contener datos personales relativos a estos interesados y su ejecución, etc.); **(d) Información financiera, fiscal y de pago** (*e.g.* datos de cuentas bancarias, datos de beneficiarios, saldos actuales e históricos de productos y servicios e historial de pagos, datos de tarjetas de crédito, domiciliación de nóminas, datos sobre / tipo de ingresos, fondos disponibles, transacciones monetarias, importe del pago, detalles de la remesa, datos de solvencia,

número de identificación fiscal, país de residencia fiscal, saldo impositivo anual, etc.); **(e) Datos de cumplimiento normativo** (*e.g.,* identificación PRP, relación MiFID o similar (*e.g.*, asociados, vínculos familiares, etc.), tipo de relación (*e.g.,* cónyuge, pariente, accionista, representantes legales, etc.), fecha de inicio y (si procede) de finalización de la relación, información relacionada con las obligaciones de prevención del fraude y de lucha contra el blanqueo de capitales (perfiles, información y puntuación / *scoring* de bases de datos de solvencia y bases de datos de riesgos, etc.); **(f) Información de voz e imagen** (*e.g.,* voz e imagen captada en fotografías, vídeo o audio en el contexto de reuniones celebradas por teléfono o videoconferencia, o con fines de seguridad, etc.); **(g) Información sobre tecnologías de la información (IT)** (*e.g.* dirección IP, número de identificación de usuario, contraseñas, registros /*logs* (incluidos los datos del perfil) de las páginas web o portales del Grupo Santander, clave de acceso a herramientas, credenciales y perfiles de seguridad, datos de autenticación informática, historial de navegación, número de identificación de dispositivo, número de identificación de publicidad, redes sociales, etc.); y **(h) Otros datos sobre la relación profesional con Grupo Santander** (*e.g.,* datos de reclamaciones, comunicaciones, preferencias de comunicación, solicitudes, etc.).

Asimismo, los Miembros del Grupo podrán tratar **categorías especiales de datos personales (incluidos datos personales relativos a condenas e infracciones penales -en el contexto de riesgos y sanciones internacionales-**) cuando sea necesario y lo exija o permita la legislación aplicable para los fines descritos en la sección siguiente.

- En relación con los datos personales de **potenciales y actuales proveedores, contratistas o suministradores** (incluidos los de sus empleados, representantes y/o agentes, según proceda):

  (a) Datos personales, profesionales y de contacto (*e.g.*, nombre, apellidos, número de teléfono, dirección de correo electrónico, dirección postal, números / documentos nacionales de identidad, cargo / puesto de trabajo, datos de la empresa, datos de contacto profesionales, etc.); **(b) Datos contractuales** (*e.g.,* datos relacionados con poderes de representación, órdenes de compra, facturas, contratos y otros acuerdos que puedan contener datos personales relativos a estos interesados, etc.); **(c) Información financiera y de pago** (*e.g.,* datos de cuentas bancarias, datos de tarjetas de crédito, datos de solvencia, etc.); **(d) Información de voz e imagen** (*e.g.,* voz e imagen captada en fotografías, vídeo o audio en el contexto de reuniones mantenidas por teléfono o videoconferencia, o con fines de seguridad (incluida la información captada a través de sistemas de entrada y cámaras de seguridad), etc.); **(e) Información sobre tecnologías de la información (IT)** (*e.g.,* dirección IP, número de identificación de usuario, contraseñas, registros / *logs* (incluidos los datos del perfil) de páginas web o portales del Grupo Santander, etc.); y **(f) Otros datos sobre la relación profesional con Grupo Santander** (*e.g.,* datos de reclamaciones, comunicaciones, etc.).

- En relación con los datos personales de **accionistas**:

  (a) Datos personales, profesionales y de contacto (*e.g.*, nombre, apellidos, sexo, fecha de nacimiento, número de teléfono, dirección de correo electrónico, dirección postal, números / documentos nacionales de identidad, cargo / puesto de trabajo, datos de la empresa, datos de contacto profesionales, número de accionista, nacionalidad / ciudadanía, país de nacimiento y residencia, etc.); **(b) Información financiera y de pago** (*e.g.* datos de cuentas bancarias, datos de tarjetas de crédito, datos de pagos, cantidad de acciones, documentos de propiedad y dividendos, transacciones monetarias, movimientos, posiciones y titulares de acciones en otras empresas, información sobre productos financieros contratados, etc.); y **(c) Información sobre tecnologías de la información (IT)** (*e.g.*, dirección IP, número de identificación de usuario, contraseñas, registros / *logs* (incluidos datos de perfil) de páginas web o portales del Grupo Santander, etc.).

- En relación con los datos personales de **usuarios de la web, usuarios finales y usuarios institucionales (incluidos los de las plataformas / páginas web / aplicaciones relacionados con las universidades, el empleo y el emprendimiento)**:

  (a) Datos personales y de contacto (*e.g.,* nombre, apellidos, fecha de nacimiento, sexo, dirección de correo electrónico, dirección postal, números de teléfono, país de residencia, nacionalidad, números nacionales de identificación, etc.); **(b) Datos profesionales y educativos** (*e.g.,* puesto / cargo, datos de la empresa, datos de contacto profesionales, historial laboral, CV, datos académicos, educación o cualificaciones, datos demográficos y socioeconómicos, conexión con proyectos empresariales o empresas, etc.); **(c) Información sobre tecnologías de la información (IT)** (*e.g.,* dirección IP, número de identificación de usuario, contraseñas, registros / *logs* sobre el uso (incluidos los datos del perfil) de páginas web o portales, registros de llamadas, etc.); **(d) Datos de navegación y uso** (*e.g.,* información recogida automáticamente de los interesados (es decir, a través de *cookies* u otras tecnologías similares) sobre su uso de páginas web / dispositivos (incluidos los perfiles), navegación web, datos de uso, etc.); y **(e) Otros datos sobre su relación con Grupo Santander** (*e.g.,* consultas, intereses, comunicaciones, etc.).

¿CON QUÉ FINES SE TRANSFIEREN DATOS PERSONALES EN VIRTUD DE ESTA POLÍTICA?

Los datos personales se transfieren entre los Miembros del Grupo a nivel mundial (principalmente Argentina, Bahamas, Brasil, Colombia, países miembros de Europa, México, Perú, Suiza, Reino Unido, Estados Unidos de América, Uruguay, etc.) en virtud de esta Política para los siguientes fines y sólo en la medida permitida por las leyes aplicables:

- Las transferencias de datos personales de **empleados actuales y pasados y otros miembros del personal (como becarios, *secondees* o autónomos)** se realizan con el fin de **(a) administrar y gestionar el personal** (*e.g.* gestión de formación, planificación y seguimiento, gestión del rendimiento, gestión de nóminas y beneficios, ascensos, planificación de la sucesión y desarrollo de la carrera profesional, administración de la movilidad interna, traslados y *secondments*, compilación y gestión de directorios de empleados actuales, organización de viajes de negocios, gestión de gastos y reembolsos de negocios, facilitación de comunicaciones, negociaciones, transacciones y conferencias comerciales, verificar el cumplimiento de las obligaciones y deberes laborales del empleado, permisos y ausencias, evaluaciones, gestionar e informar sobre asuntos disciplinarios y despidos, revisar decisiones de empleo, determinar y tomar decisiones relacionadas con la aptitud de los empleados para el trabajo y las adaptaciones del lugar de trabajo, supervisar el cumplimiento de políticas y procedimientos internos y otras actividades de supervisión exigidas por la legislación aplicable (*e.g.,* canales internos de información), incluido el cumplimiento del Código de Conducta en los Mercados de Valores o políticas similares y obligaciones relacionadas, incluida la aprobación y supervisión de las operaciones con cuentas personales, la realización de análisis y planificación de la plantilla, la realización de comprobaciones de antecedentes según exija o permita la legislación aplicable, etc.); **(b) realizar segmentaciones, estadísticas y análisis agregados** relativos a los datos de actividad de los empleados con el fin de mejorar la comprensión y fundamentar las decisiones sobre la plantilla de empleados en lo que respecta, entre otras cosas, a la captación de talento, la planificación de la carrera profesional y la planificación de la sucesión; **(c) apoyar la gestión de los servicios prestados por Grupo Santander y sus negocios** (*e.g.* gestionar y proteger los sistemas y la infraestructura informática y comunicaciones, gestionar y asignar los activos de la empresa y los recursos humanos, los equipos de oficina y otros bienes, la planificación operativa y estratégica, gestión de proyectos, continuidad del negocio, recopilación de registros de auditoría y otras herramientas de reporte, mantenimiento de registros relacionados con las actividades empresariales, elaboración de presupuestos, gestión financiera y presentación de informes, comunicaciones, gestión de fusiones, adquisiciones y reorganizaciones o enajenaciones, etc.); y **(d) cumplir con las obligaciones legales aplicables y otros requisitos** (*e.g.,*

obligaciones de protección de datos, fiscales y de seguridad social, prevención de riesgos y leyes laborales, prevención del fraude, canal de denuncias, obligaciones de mantenimiento de registros y presentación de informes, ejercicio de derechos y acciones legales, defensa en litigios, garantizar el cumplimiento con inspecciones gubernamentales y otras solicitudes del gobierno u otras autoridades públicas, responder a procesos legales como citaciones, obligaciones laborales y de seguridad social, realizar auditorías y gestionar cualquier reclamación interna o queja, etc.).

En relación con las **categorías especiales de datos personales** de los empleados **(incluidos los datos personales relativos a condenas e infracciones penales, cuando esté permitido)**, dichos datos podrán ser tratados por los Miembros del Grupo si son necesarios para el correcto logro de sus fines (*e.g.,* cumplimiento de obligaciones legales, gestión de recursos humanos, gestión de canales de denuncia, gestión de nóminas y beneficios, administración de la movilidad interna, traslados y *secondments*, realización de segmentaciones estadísticas y análisis segregados, etc.) y sólo en la medida necesaria para el cumplimiento de obligaciones y el ejercicio de derechos específicos de los Miembros del Grupo o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social (artículo 9.2(b) del RGPD) y para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, el diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria o social (artículo 9.2(h) del RGPD).

- Las transferencias de datos personales de **familiares de empleados** se realizan con fines de reubicación de empleados en el extranjero, gestión y realización de segmentaciones, estadísticas y análisis agregados, así como para supervisar el cumplimiento del Código de Conducta en los Mercados de Valores o políticas similares y obligaciones relacionadas, incluida la aprobación y supervisión de las operaciones con cuentas personales, así como la gestión de beneficios sociales en relación con los derechos de los empleados (*e.g.*, en el contexto de los seguros).

- Las transferencias de datos personales de **candidatos actuales y pasados** se realizan con el fin de gestionar las actividades de contratación nacionales / internacionales (*e.g.,* evaluar las candidaturas y tomar decisiones de contratación, comunicarse con los candidatos en relación con el proceso de contratación y / o su(s) solicitud(es), etc.).

- Las transferencias de datos personales de **clientes y consumidores potenciales y actuales** (incluidos los de sus empleados, representantes y / o agentes, usuarios autorizados y usuarios de la web) se realizan a efectos de: **(a) gestionar la relación contractual con ellos y prestarles nuestros servicios** (*e.g.*, emisión de tarjetas de pago, incluidas para usuarios autorizados en una tarjeta corporativa, oferta y gestión de nuestros servicios de pagos y de banca en línea, mantener registros para garantizar que la información sea coherente en todas las jurisdicciones, establecer acuerdos y / o tomar medidas para celebrar dichos acuerdos (procesos *KYC*), con fines comerciales y comunicaciones, transferencias entre cuentas, establecer, renovar, mantener o finalizar las relaciones comerciales, proporcionar acceso a las actividades a través de Internet y a nuestras instalaciones, mantener registros de negocio, realizar auditorías, realización de auditorías, análisis contables, financieros y económicos, realizar pagos y funciones contables relacionadas, calificación de riesgos y créditos / solvencia, etc.); **(b) gestionar y garantizar la seguridad** (*e.g.*, proteger la infraestructura informática, los equipos de oficina y otros bienes, etc.); **(c) gestionar las operaciones comerciales** (*e.g.* mantener registros de los datos de los representantes de las empresas u otros puntos de contacto, garantizar que las operaciones estén alineadas en todas las jurisdicciones, mantener registros de las reuniones y otras relaciones comerciales, operar y gestionar los sistemas informáticos y de comunicaciones, gestionar el desarrollo de productos y servicios, mejorar los productos y servicios, gestionar los activos de la empresa, planificación estratégica, gestión de proyectos, continuidad de las actividades, creación de registros de auditoría y otras herramientas de reporte, etc.); **(d) cumplir con la legislación aplicable** (*e.g.* obligaciones fiscales y de protección de datos, MiFID y adecuación e idoneidad de los productos de inversión, prevención del fraude, lucha contra el blanqueo de capitales, obligaciones de mantenimiento de registros y presentación

de informes, ejercicio de derechos y acciones legales, defensa en litigios o disputas, garantizar el cumplimiento con inspecciones gubernamentales y otras solicitudes del gobierno u otras autoridades públicas, responder a procesos legales como citaciones, etc.); y **(e) planificar y ejecutar estrategias o campañas de marketing** (*e.g.,* estudios de mercado, planificación de campañas y desarrollo de estrategias de marketing, seguimiento e información sobre el éxito de las campañas, segmentación de productos y servicios (incluida la elaboración de perfiles), cuando se cuente con el consentimiento o esté legalmente permitido, etc.).

En relación con las **categorías especiales de datos personales** de clientes (incluidos los de sus empleados, representantes y/o agentes) **(incluidos los datos personales relativos a condenas e infracciones penales)**, dichos datos podrán ser tratados por los Miembros del Grupo si fuera necesario para el correcto logro de sus fines (*e.g.* el cumplimiento de obligaciones legales, identificación de información pública sobre las prácticas de los clientes de otras entidades que puedan afectar a su relación con la empresa; garantizar que la información sea coherente en todas las jurisdicciones, garantizar el cumplimiento de inspecciones gubernamentales o judiciales y otras solicitudes de otras autoridades públicas, etc.) y sólo en la medida necesaria para el cumplimiento de las obligaciones de los Miembros del Grupo o del interesado en el ámbito de la lucha contra el blanqueo de capitales, prevención del fraude, prevención criminal y áreas afines (cuando sea necesario y requerido o permitido por la legislación aplicable).

- Las transferencias de datos personales de **potenciales y actuales proveedores, contratistas o suministradores** (incluidos los de sus empleados, representantes y/o agentes) se realizan con el fin de: **(a) gestionar la relación (pre)contractual con ellos o con su empresa** (cuando se trate de personas jurídicas) **en general** (*e.g.,* llevar a cabo comprobaciones de los niveles de estándares de calidad, análisis del nivel de riesgo de los proveedores, análisis contables, financieros y económicos, tomar medidas para suscribir los acuerdos pertinentes, ejecutar los acuerdos en vigor, realizar pagos y funciones contables relacionadas, con fines comerciales y comunicaciones, establecer, renovar, mantener o finalizar las relaciones comerciales, mantener registros comerciales, etc.); **(b) gestionar y garantizar la seguridad** (*e.g.,* proteger la infraestructura informática, los equipos de oficina y otros bienes, etc.); **(c) gestionar las operaciones comerciales** (*e.g.* operar y gestionar los sistemas informáticos y de comunicaciones, gestionar el desarrollo de productos y servicios, planificación estratégica, gestión de proyectos, continuidad de la actividad, creación de registros de auditoría y otras herramientas de reporte, mantenimiento de registros relacionados con las actividades empresariales, elaboración de presupuestos, gestión financiera y elaboración de informes, comunicaciones, etc.); y **(d) cumplir con la legislación aplicable** (*e.g.,* mercantil, fiscal, prevención del fraude, obligaciones de subcontratación cuando las realizan entidades financieras, realización de auditorías, cumplimiento con inspecciones gubernamentales y otras solicitudes del gobierno u otras autoridades públicas, ejercicio de derechos y acciones legales, defensa en litigios y gestión de cualquier reclamación interna o queja, etc.).

- Las transferencias de datos personales de **accionistas** se realizan con el fin de **(a) gestionar la relación con los accionistas** (*e.g.*, para fines comerciales y comunicaciones, establecer, renovar, mantener o finalizar las relaciones comerciales, gestionar las juntas anuales y los derechos de los accionistas, el pago de dividendos, mantener registros comerciales, proporcionar acceso a las actividades a través de Internet y a nuestras instalaciones, etc.); y **(b) cumplir con la legislación aplicable** (*e.g.*, leyes mercantiles y societarias, leyes fiscales y de valores, realización de auditorías, cumplimiento con inspecciones gubernamentales y otras solicitudes del gobierno u otras autoridades públicas, cumplimiento de las obligaciones de blanqueo de capitales, certificaciones, ejercicio de derechos y acciones legales, defensa en litigios y gestión de cualquier o reclamación interna o queja, etc.).

- Las transferencias de datos personales de **usuarios de la web, usuarios finales y usuarios institucionales (incluidos los de plataformas / páginas web / aplicaciones relacionadas con universidades, empleo y emprendimiento)** se realizan con el fin de **(a) gestionar la prestación de**

servicios en general (*e.g.*, desarrollar y proporcionar las funciones y contenidos en línea, gestionar páginas web, atender consultas y solicitudes, prestar asistencia, etc.); **(b) gestionar y garantizar la seguridad** (*e.g.,* proteger la infraestructura informática, garantizar la seguridad y la integridad de los sistemas, servidores y páginas web, etc.); **(c) gestionar las operaciones comerciales** (*e.g.,* garantizar la alineación de las operaciones en todas las jurisdicciones, mantener registros de reuniones y otras relaciones comerciales, mejorar los recursos humanos y los procesos de selección de talento a nivel mundial, etc.); **(d) planificar y ejecutar estrategias o campañas de marketing** (*e.g.,* estudios de mercado, planificación de campañas y desarrollo de estrategias de marketing, supervisión e información sobre el éxito de las campañas, selección de productos y servicios (incluida la elaboración de perfiles), cuando esté permitido por ley, etc.); **(e) gestionar las actividades de contratación nacionales e internacionales** (*e.g.*, evaluar las solicitudes y tomar decisiones de contratación, comunicarse con los candidatos en relación con el proceso de contratación y/o su(s) solicitud(es), etc.); **(f) llevar a cabo segmentaciones, estadísticas y análisis agregados** (*e.g.,* comprender cómo se utilizan los servicios, mejorar y desarrollar las funciones de la página web y de los servicios, mejorar el rendimiento y la asistencia disponible, etc.); y **(g) cumplir con la legislación aplicable** (*e.g.,* legislación mercantil, realización de auditorías, cumplimiento con inspecciones gubernamentales y otras solicitudes del gobierno u otras autoridades públicas, responder a procesos legales como citaciones, ejercicio de derechos y acciones legales, defensa en litigios y gestión de cualquier o reclamación interna o queja, etc.).

Los datos personales enumerados en esta Política también se transfieren entre los Miembros del Grupo según sea necesario para la **prestación de una amplia variedad de servicios internos entre ellos** (*e.g.*, tecnología y sistemas informáticos, servicios de *back-office*, selección y gestión de recursos humanos, auditoría interna y cumplimiento normativo, gestión del canal de denuncias, servicio central de correo para solicitudes de empleo y empleados, servicios de tecnología y procesamiento de pagos, servicios de autorización y captura de tarjetas de crédito, servicios de facturación y tarificación, destrucción de documentos, transporte de documentos, gestión de riesgos, adquisición de productos y / o servicios, facturación electrónica, gestión de marketing y comunicaciones, así como servicios de gestión y coordinación jurídica en determinados ámbitos como la protección de datos, etc.).

MÁS INFORMACIÓN

Grupo Santander ha designado DPO locales y/o Champions (tal y como estos conceptos se definirán más adelante) que dirigen los equipos locales y garantizan el cumplimiento local en diferentes entidades de todo el mundo y forman parte del Equipo de Privacidad del Grupo Santander (también definido más adelante). Si tiene alguna pregunta sobre las disposiciones de la presente Política, sus derechos en virtud de la misma o cualquier otra cuestión relacionada con la protección de datos, puede ponerse en contacto con el DPO / Champion correspondiente en la dirección que se indica a continuación. El DPO / Champion se ocupará del asunto directamente, lo remitirá a la persona o departamento apropiado dentro del Grupo Santander o escalará la cuestión a la persona / organismo correspondiente, cuando proceda.

A/A: Equipo de privacidad

Correo electrónico: Aquí encontrará una lista con las direcciones de correo electrónico pertinentes.

Si tiene alguna duda sobre la forma en que algún Miembro del Grupo ha tratado sus datos personales, existe un procedimiento específico de tramitación de reclamaciones que figura en la Parte III (véase **el Apéndice 2**).

PARTE II: OBLIGACIONES DE LOS MIEMBROS DEL GRUPO

La Parte II de esta Política se divide en tres secciones:

- La Sección A aborda los principios de protección de datos básicos alineados con aquellos de la Normativa Europea de Protección de Datos que debe respetar un Miembro del Grupo.

- La Sección B trata de los compromisos prácticos contraídos por los Miembros del Grupo con las autoridades de control competentes en relación con esta Política.

- La Sección C describe los derechos de terceros beneficiarios que los Miembros del Grupo han concedido a los interesados en virtud de la Parte II de esta Política.

SECCIÓN A: PRINCIPIOS BÁSICOS

REGLA 1 - LICITUD Y LEALTAD

Regla 1A – Los Miembros del Grupo cumplirán esta Política y cualquier Ley Local de PD Aplicable de forma armonizada.

Como organizaciones, los Miembros del Grupo cumplirán, según lo dispuesto a continuación, toda la legislación aplicable en materia de datos personales (*e.g.*, en Europa, la Normativa Europea de Protección de Datos) y se asegurarán de que, cuando se traten datos personales, se haga de conformidad con esta Política y con la Ley Local de PD Aplicable en materia de protección de datos.

Cuando esta Política resulta de aplicación y:

- no existe una Ley Local de PD Aplicable, o la ley no responde a las exigencias establecidas por las Reglas de esta Política, la posición de los Miembros del Grupo consistirá en tratar los datos personales sujetos a la presente Política de acuerdo con las Reglas establecidas en la misma;

- la Ley Local de PD Aplicable exige un nivel de protección superior al previsto en la presente Política, el nivel de protección superior prevalecerá sobre la presente Política, siempre que se sigan respetando los derechos y obligaciones establecidos en esta Política; o

- la Ley Local de PD Aplicable impide a los Miembros del Grupo cumplir con sus obligaciones en virtud de esta Política, o tiene un efecto sustancial sobre su capacidad para hacerlo, los Miembros del Grupo seguirán el procedimiento establecido en la Regla 13.

Regla 1B - Los Miembros del Grupo se asegurarán de que el tratamiento de sus datos personales sea lícito y leal y de que exista una base jurídica para el tratamiento de los datos personales, cuando sea necesario.

Los Miembros del Grupo se asegurarán de que el tratamiento de sus datos personales sea lícito y leal, y de que exista una base jurídica para el tratamiento de los datos personales cuando sea necesario. De acuerdo con la Normativa Europea de Protección de Datos, los Miembros del Grupo sólo tratarán datos personales cuando:

- el interesado haya dado su consentimiento para el tratamiento de sus datos personales y dicho consentimiento cumpla con los requisitos exigidos por la Normativa Europea de Protección de Datos (es decir, debe ser libre, específico, informado e inequívoco); o bien

- sea necesario para la ejecución de un contrato en el que el interesado es parte, o para la aplicación a petición de este de medidas precontractuales; o

- sea necesario para el cumplimiento de una obligación legal aplicable al Miembro del Grupo (siempre que dicha legislación cumpla con los requisitos establecidos en la Regla 13 de la presente Política, cuando resulte de aplicación); o

- sea necesario para proteger intereses vitales del interesado o de otra persona física; o

- sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a un Miembro del Grupo (siempre que dicha misión esté prevista en una ley que cumpla con los requisitos establecidos en la Regla 13 de la presente Política, cuando resulte de aplicación); o

- sea necesario para la satisfacción de intereses legítimos perseguidos por un Miembro del Grupo o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado.

Cuando el tratamiento de datos personales se refiera a condenas e infracciones penales o a medidas de seguridad conexas, los Miembros del Grupo no llevarán a cabo dicho tratamiento si no es bajo la supervisión de las autoridades públicas o cuando lo autorice una ley que establezca garantías adecuadas para los derechos y libertades de los interesados de conformidad con las bases jurídicas anteriormente mencionadas.

Regla 1C - Sin perjuicio de lo dispuesto en la Regla 1B anterior, queda prohibido el tratamiento de categorías especiales de datos personales, salvo que sea de aplicación una excepción como las previstas en la Normativa Europea de Protección de Datos.

El tratamiento de categorías especiales de datos personales sólo está permitido por determinados motivos:

- el Miembro del Grupo ha obtenido el consentimiento explícito para el tratamiento de cualquier categoría especial de datos personales relativa a un interesado con uno o más de los fines especificados, a menos que una ley establezca que la prohibición de tratar datos de categoría especial no puede ser levantada por el interesado; o

- el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Miembro del Grupo o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice la ley o un convenio colectivo con arreglo a la legislación que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses de los interesados; o

- el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; o

- el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados; o

- el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; o
- el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial; o
- el tratamiento es necesario por razones de un interés público esencial, sobre la base de la ley, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado; o
- el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o la gestión de los sistemas y servicios de asistencia sanitaria y social sobre la base de la ley, siempre que el tratamiento sea realizado por un profesional o bajo su responsabilidad sujeto a obligaciones de confidencialidad de acuerdo con la ley o con las normas establecidas por organismos nacionales competentes; o
- el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de una ley que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional; o
- el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sobre la base de una ley, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Regla 1D - Los Miembros del Grupo evaluarán el impacto de cualquier tratamiento de datos personales que implique un alto riesgo para los derechos y libertades de los interesados.

Las Entidades Exportadoras, cuando actúen como responsables del tratamiento, evaluarán la necesidad y proporcionalidad de cualquier nuevo tratamiento de datos personales y, en caso de que implique un alto riesgo para los derechos y libertades de los interesados, llevarán a cabo una evaluación de impacto relativa a la protección de datos de conformidad con la Normativa Europea de Protección de Datos. En caso de que la evaluación de impacto relativa a la protección de datos muestre que el tratamiento entrañará un alto riesgo para los interesados, las Entidades Exportadoras deberán consultar a las autoridades de control competentes antes de iniciar el tratamiento si no se han adoptado medidas para mitigar el riesgo.

REGLA 2 - GARANTIZAR LA TRANSPARENCIA Y TRATAR LOS DATOS PERSONALES SOLO PARA UN FIN CONOCIDO

Regla 2A - Los Miembros del Grupo informarán a los interesados sobre cómo se tratarán sus datos.

Los Miembros del Grupo se asegurarán de que siempre se informe a los interesados de forma clara y exhaustiva (normalmente mediante una política del tratamiento leal) sobre cómo se tratarán sus datos personales. El Miembro del Grupo correspondiente facilitará la información de conformidad con lo exigido por la Normativa Europea de Protección de Datos, que incluirá como mínimo lo siguiente:

- la identidad y los datos de contacto del responsable del tratamiento, incluidos los datos de contacto del delegado de protección de datos y del representante, según proceda;

- la finalidad y la base jurídica del tratamiento, incluida una explicación sobre cualquier tratamiento basado en intereses legítimos y cualquier finalidad compatible nueva o diferente;

- los destinatarios o categorías de destinatarios de los datos personales;

- información sobre las garantías establecidas para proteger los datos personales cuando se transfieren internacionalmente y cómo acceder u obtener una copia de dichas garantías. En el caso de transferencias de datos personales entre una Entidad Exportadora y una Entidad Importadora basadas en la presente Política, la información facilitada incluirá una referencia a la presente Política y a la forma de acceder a ella;

- el periodo durante el cual se almacenarán los datos personales o los criterios utilizados para determinar dicho periodo;

- información detallada sobre los derechos de los interesados, incluido el derecho de acceso, rectificación, supresión, limitación, oposición, portabilidad, el derecho a retirar el consentimiento (cuando el tratamiento se base en el consentimiento) y el derecho a presentar una reclamación ante una autoridad de control;

- si la comunicación de la información es un requisito legal o contractual, y las consecuencias de no facilitar los datos personales en tales circunstancias; e

- información sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en los casos en que dichas decisiones produzcan efectos jurídicos en el interesado o le afecten significativamente de modo similar, o se basen en categorías especiales de datos personales, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Los requisitos de la Ley Local de PD Aplicable donde se recaben los datos personales determinará si debe facilitarse información adicional a los interesados.

Esta información se facilitará cuando los Miembros del Grupo obtengan los datos personales del interesado o en un plazo permitido por la Normativa Europea de Protección de Datos.

Cuando los Miembros del Grupo obtengan los datos personales del interesado de una fuente distinta de dicho interesado, el Miembro del Grupo correspondiente proporcionará esta información al interesado, junto con información sobre la fuente y las categorías de datos personales recibidos de terceros, como se indica a continuación:

- dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un (1) mes;

- si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado; o

- si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

Los Miembros del Grupo seguirán esta Regla 2A a menos que no proporcionar información esté específicamente permitido por la Normativa Europea de Protección de Datos.

Regla 2B - Los Miembros del Grupo sólo obtendrán y tratarán datos personales para aquellos fines que sean conocidos por el interesado, o que sean compatibles con sus expectativas y sean pertinentes para los Miembros del Grupo.

La Regla 1A establece que los Miembros del Grupo cumplirán toda la legislación aplicable relativa al tratamiento de datos personales (siempre que dicha legislación cumpla con los requisitos establecidos en la Regla 13 de la presente Política, cuando resulte de aplicación). Esto significa que los Miembros del Grupo recabarán los datos personales con fines determinados, explícitos y legítimos y no tratarán posteriormente dichos datos personales de manera incompatible con dichos fines.

Los Miembros del Grupo identificarán y darán a conocer los fines para los que se tratarán los datos personales (incluidos los usos ulteriores y comunicaciones de los datos) de conformidad con la Regla 2A.

Regla 2C - Los Miembros del Grupo sólo podrán tratar datos personales para un fin distinto o nuevo si es compatible con el fin para el que se recabaron.

Si un Miembro del Grupo recaba datos personales para un fin determinado de conformidad con la Regla 2A (comunicado al interesado a través de la correspondiente política del tratamiento leal) y según lo descrito en la Regla 2B, y, posteriormente, el Miembro del Grupo desea tratar los datos personales para un fin diferente o nuevo, no tratará dichos datos personales de forma incompatible con el fin para el que fueron recabados, a menos que dicho tratamiento ulterior se base en el consentimiento del interesado o lo exija la ley (siempre que dicha ley cumpla con los requisitos establecidos en la Regla 13 de la presente Política, cuando resulte de aplicación).

REGLA 3 - GARANTIZAR LA CALIDAD DE LOS DATOS

Regla 3A - Los Miembros del Grupo mantendrán los datos personales exactos y actualizados.

Para garantizar que los datos personales en poder de los Miembros del Grupo sean exactos y estén actualizados, los Miembros del Grupo animan activamente a los interesados a que les informen cuando se produzcan cambios en sus datos personales. Los Miembros del Grupo tomarán medidas razonables para garantizar que los datos personales que sean inexactos con respecto a los fines para los que se tratan, se supriman o rectifiquen sin dilación.

Regla 3B - Los Miembros del Grupo sólo conservarán los datos personales durante el tiempo que sea necesario para los fines para los que se tratan.

Los Miembros del Grupo cumplirán con la normativa aplicable a cada Miembro del Grupo y las políticas y procedimientos de retención de datos del Grupo Santander, revisados y actualizados periódicamente. Esto significa, entre otras cosas, que los Miembros del Grupo suprimirán o bloquearán, según el caso, los datos personales que ya no sean necesarios para los fines para los que se recogieron y trataron posteriormente.

Regla 3C - Los Miembros del Grupo sólo tratarán los datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan.

Los Miembros del Grupo sólo tratarán los datos personales que sean necesarios para el correcto cumplimiento de los fines para los que son tratados.

REGLA 4 - ADOPTAR MEDIDAS DE SEGURIDAD APROPIADAS

Regla 4A - Los Miembros del Grupo cumplirán con las políticas de seguridad de tecnologías de la información del Grupo Santander.

Los Miembros del Grupo implementarán las medidas técnicas y organizativas apropiadas para proteger los datos personales contra la destrucción, pérdida o alteración accidental o ilícita o la comunicación o acceso no autorizados, en particular cuando el tratamiento implique la transmisión de datos personales a través de una red, y contra cualquier otra forma ilícita de tratamiento. A tal fin, los Miembros del Grupo cumplirán los requisitos de las políticas de seguridad vigentes en el Grupo Santander, revisadas y actualizadas periódicamente, junto con cualesquiera otros procedimientos de seguridad pertinentes para un área de negocio o departamento. Teniendo en cuenta el estado de la técnica y el coste de su implementación, dichas medidas garantizarán un nivel de seguridad adecuado a los riesgos que presente el tratamiento y a la naturaleza de los datos que deban protegerse.

Regla 4B - Los Miembros del Grupo han implementado una política de notificación de brechas de seguridad.

Los Miembros del Grupo han implantado procedimientos de respuesta a violaciones de seguridad de los datos personales (revisados y actualizados periódicamente) que establecen el proceso que se debe seguir en caso de violación de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, (una "**Brecha de Seguridad**").

En particular, en caso de una Brecha de Seguridad, la persona que tenga conocimiento de la brecha dentro del Miembro del Grupo correspondiente lo notificará, sin demora indebida, al:

- DPO o Champion pertinente, a través del Departamento de Control del Riesgo Operativo (según proceda);
- Miembro del Grupo que actúa como responsable del tratamiento cuando el Miembro del Grupo pertinente actúa como encargado del tratamiento; y
- Miembro Responsable de las BCR.

El DPO o Champion correspondiente evaluará, con la ayuda de la Oficina Corporativa de PD, cuando sea necesario, si la Brecha de Seguridad debe notificarse a la autoridad de control competente. En tal caso, el DPO o el Champion, según proceda, procederá a comunicar la Brecha de Seguridad a la autoridad de control competente en el plazo requerido (de conformidad con la Normativa Europea de Protección de Datos, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella).

También se notificará a los interesados sin dilación indebida en los casos en que sea probable que la Brecha de Seguridad entrañe un alto riesgo para sus derechos y libertades, a menos que dicha notificación no sea necesaria en virtud de la Normativa Europea de Protección de Datos.

En línea con lo anterior, las Brechas de Seguridad sufridas por los Miembros del Grupo, que comprenderán los hechos, los efectos de dichas incidencias y las medidas correctivas adoptadas, se registrarán también en Heracles, el registro de incidencias de seguridad del Grupo Santander (incluidas las Brechas de Seguridad) que estará a disposición de la autoridad de control competente que lo solicite.

Regla 4C - Los Miembros del Grupo se asegurarán de que los proveedores de servicios y otras entidades que traten datos personales en su nombre también adopten medidas de seguridad apropiadas y equivalentes.

Los Miembros del Grupo que utilicen un proveedor de servicios (que actúe como encargado del tratamiento) que tenga acceso a los datos personales de los interesados (e.g., un gestor de nóminas), impondrán al encargado del tratamiento obligaciones contractuales por escrito que cumplan los requisitos de la Normativa Europea de Protección de Datos en forma de un acuerdo de encargo vinculante. Dicho acuerdo deberá prever, como mínimo, lo siguiente:

- El objeto y la duración del tratamiento, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y las categorías de interesados;

- Obligaciones y derechos del responsable del tratamiento;

- Las siguientes obligaciones para la entidad que actúa como encargada del tratamiento:

    - Tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable del tratamiento, inclusive con respecto a las transferencias de datos personales a un tercer país o a una organización internacional, salvo que esté obligado a ello en virtud de una ley que se aplique al encargado del tratamiento (siempre que dicha ley cumpla con los requisitos establecidos en la Regla 13 de la presente Política, cuando resulte de aplicación). En tal caso, el encargado del tratamiento informará al responsable del tratamiento de esa exigencia legal previa al tratamiento, salvo que dicha ley lo prohíba por razones importantes de interés público;

    - Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sometidas a una obligación de confidencialidad de naturaleza estatutaria;

    - Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que entraña el tratamiento de los datos personales;

    - No contratar a otro encargado del tratamiento en relación con los datos personales sin la autorización previa por escrito, específica o general, del responsable del tratamiento y sin firmar, según el caso, un contrato por escrito con el otro encargado del tratamiento que contenga las mismas obligaciones en materia de protección de datos que las establecidas en el contrato u otro acto jurídico entre el responsable del tratamiento y el encargado del tratamiento (en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones de la Normativa Europea de Protección de Datos);

    - Asistir al responsable del tratamiento, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados (descritos con más detalle en la Regla 5);

    - Ayudar al responsable del tratamiento a garantizar el cumplimiento de las obligaciones relacionadas con la implementación de medidas de seguridad apropiadas, la realización de evaluaciones de impacto relativas a la protección de datos y las consultas correspondientes a

las autoridades de control competentes; y las obligaciones de notificación de Brechas de Seguridad a las autoridades de control competentes y a los interesados (cuando proceda);

- A elección del responsable del tratamiento, suprimir o devolver todos los datos personales al responsable del tratamiento una vez finalice la prestación de los servicios de tratamiento, y suprimir las copias existentes, a menos que se requiera la conservación de los datos personales en virtud de una ley;

- Poner a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones como encargado del tratamiento y permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable del tratamiento u otro auditor autorizado por dicho responsable del tratamiento; y

- Informar inmediatamente al responsable del tratamiento si, en su opinión, una instrucción infringe una ley.

REGLA 5 - GARANTIZAR LOS DERECHOS DE LOS INTERESADOS

Regla 5 - Los Miembros del Grupo atenderán las solicitudes de los interesados relativas a sus derechos en materia de protección de datos (incluidos el acceso, rectificación, supresión, limitación o transmisión de datos personales, u oposiciones al tratamiento de datos personales, así como a la revocación del consentimiento).

Previa solicitud, los interesados tienen derecho a solicitar los siguientes derechos prescritos por la Normativa Europea de Protección de Datos:

- derecho de acceso, que consiste en facilitar información sobre los datos personales que se dispongan del interesado y confirmar si se están tratando sus datos personales;

- derecho de rectificación, por el que el interesado tendrá derecho a obtener la rectificación de cualquier dato personal que pudiera ser inexacto o incompleto;

- derecho de supresión o "derecho al olvido", por el que el interesado tendrá derecho a que se supriman sus datos personales cuando se den determinadas circunstancias (como las previstas en el artículo 17 del RGPD);

- derecho a la limitación del tratamiento, por el que el interesado tendrá derecho a solicitar la limitación del tratamiento de sus datos personales cuando concurran determinadas circunstancias (como las previstas en el artículo 18 del RGPD);

- derecho a que se notifique a cada uno de los destinatarios a los que se hayan comunicado los datos personales cualquier rectificación o supresión de los datos personales o la limitación de su tratamiento, salvo que sea imposible o exija un esfuerzo desproporcionado. El interesado también podrá solicitar que se le informe acerca de dichos destinatarios;

- derecho a la portabilidad de los datos, en virtud del cual el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, y a transmitirlos a otro responsable del tratamiento;

- derecho de oposición, por el que el interesado tendrá derecho a oponerse al tratamiento de sus datos personales para un fin determinado, incluido el tratamiento con fines de mercadotecnia directa y la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia;

- derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o que le afecte significativamente de modo similar (cuando proceda); y

- derecho a revocar en cualquier momento el consentimiento dado para un tratamiento determinado.

REGLA 6 - GARANTIZAR UNA PROTECCIÓN ADECUADA DE LAS TRANSFERENCIAS Y TRANSFERENCIAS ULTERIORES

Regla 6 - Los Miembros del Grupo no transferirán datos personales a terceros fuera de Europa sin garantizar una protección adecuada de los datos personales de acuerdo con las normas establecidas por esta Política y de conformidad con la Normativa Europea de Protección de Datos.

Las transferencias y las transferencias ulteriores de datos personales de Miembros del Grupo sujetos a la Normativa Europea de Protección de Datos a terceros fuera de Europa no están permitidas sin tomar las medidas adecuadas, tal y como exige la Normativa Europea de Protección de Datos.

Estos pasos pueden incluir, entre otros:

- confirmar que el tercero está situado en un país que, según la Comisión Europea, ofrece un nivel adecuado de protección de los datos personales transferidos; o

- suscribir cláusulas contractuales tipo adecuadas u otros mecanismos previstos en la Normativa Europea de Protección de Datos;

- garantizar que la transferencia es necesaria para: (i) la ejecución de un contrato entre el interesado y el Miembro del Grupo que transfiere los datos o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado; (ii) la celebración o ejecución de un contrato celebrado en interés del interesado entre el Miembro del Grupo que transfiere los datos y otra parte; (iii) razones importantes de interés público reconocidas en el Derecho de la Unión o en el Derecho del Estado miembro al que esté sujeto el responsable del tratamiento; (iv) el formulación, ejercicio o defensa de un derecho en un procedimiento judicial; (v) la protección de los intereses vitales del interesado o de otra persona física, cuando el interesado no esté en condiciones de dar su consentimiento; o (vi) la obtención del consentimiento explícito de los interesados, tras haber sido informados de los posibles riesgos de dicha transferencia debido a la ausencia de una decisión de adecuación y de garantías apropiadas.

SECCIÓN B: COMPROMISOS PRÁCTICOS

REGLA 7 - CUMPLIMIENTO Y RESPONSABILIDAD PROACTIVA

Regla 7A - Los Miembros del Grupo serán responsables del cumplimiento de esta Política y podrán demostrarlo, y dispondrán del personal y el apoyo adecuados para garantizar y supervisar el cumplimiento de esta Política en todo el negocio.

Grupo Santander cuenta con una estructura organizativa de privacidad encargada de decidir, coordinar, implementar y supervisar cualquier evento que pueda tener lugar dentro de Grupo Santander en materia de protección de datos (el "**Equipo de Privacidad**"). La estructura de privacidad del Grupo Santander está compuesta por:

- **Oficina Corporativa de Protección de Datos** ("**Oficina Corporativa de PD**"): Órgano corporativo encargado de fijar los criterios generales y elaborar las políticas corporativas de protección de datos aplicables. Se configura, junto con el equipo de Riesgos No Financieros, como una segunda línea de defensa (2LoD) global que se encarga de supervisar la gestión de las actividades relacionadas con la privacidad llevadas a cabo por la primera línea de defensa (1LoD) y de asegurar una adecuada gestión del riesgo de acuerdo con el apetito de riesgo del Grupo Santander.

  Como 2LoD global, la Oficina Corporativa de PD y el equipo de Riesgos No Financieros asumen una serie de funciones sobre todas las entidades del Grupo Santander sujetas a la Normativa Europea de Protección de Datos, entre ellas principalmente:

  - Supervisión y control del cumplimiento: (i) supervisar el cumplimiento en materia de protección de datos del Grupo Santander; (ii) reportar información consolidada a la alta dirección del Grupo Santander; (iii) ser punto de contacto global, a través de los distintos DPOs (o figuras similares) locales, con las autoridades de control competentes; (iv) análisis de impacto, junto con las funciones de negocio y soporte que correspondan, de los incidentes de seguridad a nivel global; (v) análisis y reporte global de riesgos en materia de protección de datos; y (vi) facilitar los criterios corporativos y ser punto de contacto en la corporación para los DPOs / Champions de las entidades (ver más abajo).

  - Función de apoyo a los DPOs y Champions del Grupo Santander (unidades / entidad(es) corporativas y entidades locales). Principalmente proporcionando asesoramiento especializado en materia de regulación y apoyo en el desempeño de los departamentos locales de privacidad.

- **Estructura & Gobernanza**

  - **Banco Santander (Corporación)**: dos figuras principales apoyan y reportan a la Oficina Corporativa de PD:

    - **DPO de Banco Santander** (designado formalmente ante la autoridad de control española): sus funciones dentro de la matriz, que el DPO desempeña de forma independiente, se limitan a las descritas en el RGPD que requieren, entre otras, su participación en el diálogo con la autoridad de control española. Sin perjuicio de las obligaciones de información y apoyo del DPO con respecto a la Oficina Corporativa de PD, el DPO depende directamente del más alto nivel directivo de Banco Santander.

    - **Unidades corporativas**: unidades designadas en toda la organización. Sus principales funciones y responsabilidades consisten en: (a) ejecutar y resolver en primera instancia los asuntos relacionados con los datos personales; (b) informar y asesorar a los responsables, encargados y empleados sobre cómo cumplir la normativa aplicable en materia de protección de datos; (c) supervisar el cumplimiento de la normativa de protección de datos; (d) ser el punto de contacto interno como área de apoyo de primer

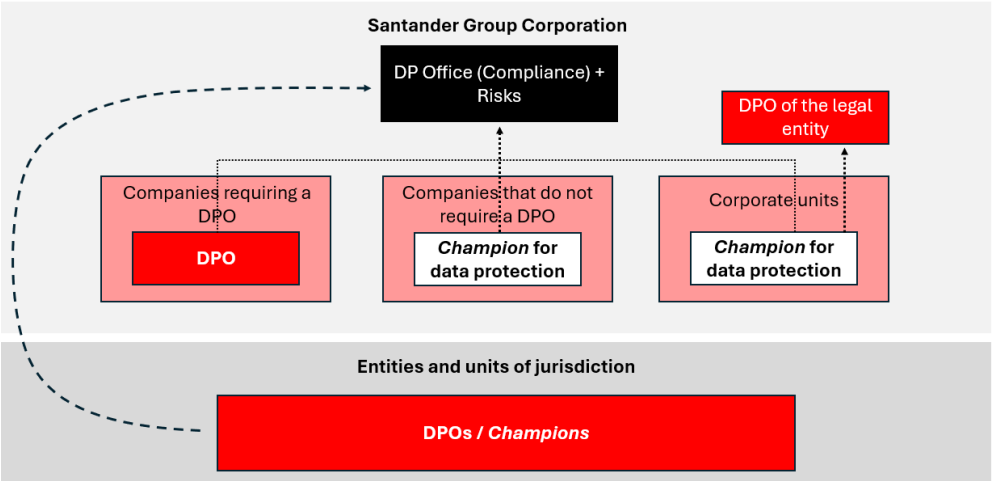
nivel; (e) canalizar las consultas y solicitudes de apoyo a la Oficina Corporativa de PD e informar los indicadores de gestión.

- **Unidades locales**: también hay dos figuras que reportan a la Oficina Corporativa de PD:

  - **DPO (o figura local similar)**: cuando así lo exija la Ley Local de PD Aplicable, se designará un DPO (o figura local similar). Sus principales funciones y responsabilidades pueden incluir: (a) ser punto de contacto con la autoridad de control pertinente y con las partes interesadas; (b) cooperación con la autoridad de control pertinente; (c) asesoramiento en materia de protección de datos; (d) seguimiento y supervisión; (e) formación; (f) asesoramiento sobre evaluaciones de impacto en materia de protección de datos; (g) realización de consulta(s) previa(s) a la autoridad de control pertinente; (h) supervisión de los registros de las actividades de tratamiento; (i) asesoramiento sobre la notificación de Brechas de Seguridad; (j) asesoramiento sobre la gestión de terceros; y (k) supervisión del ejercicio de los derechos de los interesados.

  - **Champions o figura local similar (e.g., responsable de privacidad):** cuando no se requiera un DPO según la Ley Local de PD Aplicable o cuando, debido al tamaño y/o complejidad de una entidad, ésta requiera un gran número de DPOs o figura local similar, la Oficina Corporativa de PD podrá contar con el apoyo y reporte de Champions locales o figuras similares (e.g., responsable de privacidad). Sus funciones y responsabilidades son muy similares a las de los DPO o figuras similares, salvo en lo que respecta a las comunicaciones con las autoridades de control (en las que no participan).

A continuación, encontrará un diagrama que muestra la estructura organizativa y de relaciones entre las mencionadas figuras responsables de la protección de datos en el Grupo Santander:



Regla 7B - Los Miembros del Grupo implementarán las medidas técnicas y organizativas adecuadas, desde el diseño y por defecto, para permitir y facilitar el cumplimiento de la Política en la práctica.

Teniendo en cuenta el estado de la técnica y el coste de su implementación, así como el ámbito, la naturaleza, el contexto y los fines del tratamiento, los Miembros del Grupo implementarán medidas técnicas y

organizativas apropiadas que cumplan los principios de la protección de datos desde el diseño y por defecto, tal y como exige la Normativa Europea de Protección de Datos. Los Miembros del Grupo integrarán dichas medidas en el tratamiento a la hora de determinar los medios del tratamiento, y el momento del tratamiento en sí para facilitar la protección de los datos personales que se estén tratando, y con el fin de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Regla 7C - Los Miembros del Grupo que traten datos personales mantendrán un registro escrito (inclusive en formato electrónico) de sus actividades de tratamiento y pondrán dicho registro a disposición de las autoridades de control competentes que lo soliciten.

Los registros de tratamiento de datos mantenidos por los Miembros del Grupo que actúen como responsables del tratamiento, contendrán:

- el nombre y los datos de contacto del Miembro del Grupo y, en su caso, del corresponsable del tratamiento, del representante del responsable del tratamiento y del delegado de protección de datos;
- los fines para los que se tratan los datos personales;
- una descripción de las categorías de interesados sobre los que se tratan datos personales y las categorias datos personales tratados;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- los datos del tercer país o terceros países a los que se transfieren los datos personales, incluida la identificación de dicho tercer país u organización internacional y la documentación de las garantías adecuadas aplicadas para legitimar dichas transferencias (a menos que el país haya sido declarado adecuado en virtud de la Normativa Europea de Protección de Datos);
- cuando sea posible, el período durante el cual se conservarán los datos personales; y
- cuando sea posible, una descripción general de las medidas de seguridad técnicas y organizativas implementadas para proteger los datos personales.

Los registros de tratamiento de datos mantenidos por los Miembros del Grupo que actúen como encargados del tratamiento para un Miembro del Grupo que sea el responsable del tratamiento, contendrán:

- el nombre y los datos de contacto del Miembro del Grupo y de cada responsable del tratamiento por cuenta del cual actúe el encargado del tratamiento y, en su caso, del representante del responsable del tratamiento o del encargado del tratamiento, así como del delegado de protección de datos;
- las categorías de tratamiento efectuadas por cuenta de cada responsable del tratamiento;
- datos del tercer país o terceros países a los que se transfieren los datos personales, incluida la identificación de dicho tercer país u organización internacional y la documentación de las garantías adecuadas aplicadas para legitimar dichas transferencias (a menos que el país haya sido declarado adecuado en virtud de la Normativa Europea de Protección de Datos); y
- cuando sea posible, una descripción general de las medidas de seguridad técnicas y organizativas implementadas para proteger los datos personales.

Los registros de tratamiento de datos mantenidos por los Miembros del Grupo se harán por escrito, inclusive en formato electrónico, y se pondrán a disposición de las autoridades de control competentes a petición de éstas.

REGLA 8 - FORMACIÓN

Regla 8 - Los Miembros del Grupo proporcionarán formación adecuada a los empleados que tengan acceso permanente o regular a datos personales y/o que participen en el tratamiento de datos personales o en el desarrollo de herramientas utilizadas para tratar dichos datos personales.

Los Miembros del Grupo proporcionarán una formación adecuada y actualizada a los empleados que tengan acceso permanente o regular a datos personales y/o que participen en el tratamiento de dichos datos personales o en el desarrollo de herramientas utilizadas para el tratamiento de dichos datos personales. Dicha formación se impartirá al menos una vez cada dos años y abarcará, entre otros aspectos, los procedimientos de gestión de las solicitudes de acceso a datos personales por parte de las autoridades públicas.

REGLA 9 - AUDITORÍA

Regla 9 - Los Miembros del Grupo cumplirán con el Programa de Auditoría que figura en el Apéndice 1.

Los Miembros del Grupo cumplirán con el Programa de Auditoría realizando auditorías internas periódicas y permitiendo auditorías externas, cuando sea necesario, de acuerdo con el proceso de evaluación formal estipulado en el Programa de Auditoría. El resultado de dichas auditorías se comunicará de conformidad con lo previsto en el Apéndice 1.

REGLA 10- TRAMITACIÓN DE RECLAMACIONES

Regla 10 - Los Miembros del Grupo cumplirán con el Procedimiento de Tramitación de Reclamaciones que figura en el Apéndice 2.

Los Miembros del Grupo cumplirán con el Procedimiento de Tramitación de Reclamaciones establecido en el Apéndice 2 con el fin de gestionar adecuadamente las reclamaciones de los interesados y proteger el tratamiento de datos personales por parte de los Miembros del Grupo. Los Miembros del Grupo también permitirán el ejercicio de los derechos de terceros beneficiarios, tal como se establece en la Sección C de esta Política.

REGLA 11 - COOPERACIÓN CON LAS AUTORIDADES DE CONTROL COMPETENTES

Regla 11 - Los Miembros del Grupo cumplirán con el Procedimiento de Cooperación establecido en el Apéndice 3.

Los Miembros del Grupo cumplirán con el Procedimiento de Cooperación establecido en el Apéndice 3 y cooperarán con las autoridades de control competentes, aceptando ser auditados e inspeccionados por ellas (incluso *in situ*, cuando sea necesario), en relación con esta Política; así como a tener en cuenta sus consejos y acatar sus decisiones sobre cualquier cuestión relacionada con esta Política.

REGLA 12 - ACTUALIZACIÓN DE LAS REGLAS

Regla 12 - Los Miembros del Grupo cumplirán con el Procedimiento de Actualización establecido en el Apéndice 4.

Los Miembros del Grupo cumplirán con el Procedimiento de Actualización establecido en el Apéndice 4 y comunicarán sin demora indebida cualquier actualización de esta Política y de la lista de Miembros del Grupo a las autoridades de control competentes, a los interesados afectados y a los Miembros del Grupo, según sea necesario.

REGLA 13 - ACTUACIÓN EN CASO DE QUE LA LEGISLACIÓN NACIONAL AFECTE AL CUMPLIMIENTO DE LA POLÍTICA

Regla 13A - Los Miembros del Grupo se comprometen a utilizar esta Política como instrumento para las transferencias a Entidades Importadoras únicamente cuando hayan evaluado debidamente que la legislación y las prácticas del país de las Entidades Importadoras (incluidos los requisitos de divulgación de datos personales o las medidas que autorizan el acceso por parte de las autoridades públicas) no les impiden cumplir con sus obligaciones en virtud de esta Política.

Los Miembros del Grupo utilizarán esta Política como instrumento para salvaguardar las transferencias internacionales únicamente cuando hayan evaluado que la legislación y las prácticas de los terceros países de destino pertinentes, incluidos los requisitos de divulgación de datos personales o las medidas que autorizan el acceso por parte de las autoridades públicas, no les impiden cumplir sus obligaciones en virtud de esta Política. Esto se basará en el entendimiento de que las leyes y prácticas que respetan la esencia de los derechos y libertades fundamentales y no exceden lo que es necesario y proporcionado en una sociedad democrática, no entran en contradicción con la Política.

Al evaluar la legislación y las prácticas de los terceros países que puedan afectar al respeto de los compromisos contenidos en la presente Política, los Miembros del Grupo tendrán debidamente en cuenta, en particular, los siguientes elementos:

(i) las circunstancias concretas de las transferencias o conjunto de transferencias, y de cualquier transferencia ulterior prevista dentro del mismo tercer país o a otro tercer país, en particular:

- los fines para los que se transfieren y tratan los datos (*e.g.*, comercialización, recursos humanos, almacenamiento, asistencia informática, etc.);
- los tipos de entidades que participan en el tratamiento (la Entidad Importadora y cualquier otro destinatario de una transferencia ulterior);
- el sector económico en el que se produce la transferencia o el conjunto de transferencias;
- las categorías y el formato de los datos personales transferidos;
- la ubicación del tratamiento, incluido el almacenamiento; y
- los canales de transmisión utilizados.

(ii) las leyes y prácticas de los terceros países de destino pertinentes a la luz de las circunstancias de la transferencia. Entre ellas pueden figurar: (a) las que exigen la divulgación de datos a las autoridades

públicas o autorizan el acceso por parte de dichas autoridades; (b) las que prevén el acceso a estos datos durante el tránsito entre los países de las Entidades Exportadoras y los países de las Entidades Importadoras; y (c) las limitaciones y garantías aplicables.

(iii) todas las garantías contractuales, técnicas u organizativas pertinentes aportadas para complementar las garantías previstas en la presente Política. Esto incluye las medidas aplicadas durante la transferencia y el tratamiento de los datos personales en los países de destino.

Cuando deban establecerse garantías adicionales a las previstas en la presente Política, se informará e implicará en la evaluación al Miembro Responsable de las BCR y al DPO o Champion correspondiente, según el caso. Los Miembros del Grupo documentarán adecuadamente dicha evaluación, así como las medidas complementarias elegidas y aplicadas. Pondrán dicha documentación a disposición de la autoridad de control competente a petición de ésta.

Las Entidades Importadoras notificarán sin demora a las Entidades Exportadoras si, al utilizar esta Política como instrumento para las transferencias, y mientras dure la adhesión, tienen razones para creer que están o han estado sujetas a leyes o prácticas que les impedirían cumplir sus obligaciones en virtud de la misma. Esto incluye la imposibilidad de cumplir con sus obligaciones a raíz de un cambio en la legislación del tercer país pertinente o de una medida (como una solicitud de revelar información). Esta información también deberá facilitarse al Miembro Responsable de las BCR.

Una vez verificada dicha notificación, la Entidad Exportadora correspondiente, junto con el Miembro Responsable de las BCR y el DPO o Champion correspondiente, según sea el caso, se comprometen a identificar con prontitud las medidas complementarias (*e.g.,* medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que deberán adoptar la Entidad Exportadora y/o la Entidad Importadora a fin de permitirles cumplir sus obligaciones en virtud de la presente Política. Lo mismo se hará si una Entidad Exportadora tiene razones para creer que una Entidad Importadora ya no puede cumplir sus obligaciones en virtud de la presente Política.

Cuando la Entidad Exportadora correspondiente, junto con el Miembro Responsable de las BCR y el DPO o Champion correspondiente, según sea el caso, evalúe que la Política -incluso si va acompañada de medidas complementarias- no puede cumplirse para una transferencia o conjunto de transferencias o si recibe instrucciones de la autoridad de control competente; se compromete a suspender la transferencia o conjunto de transferencias en cuestión, así como todas las transferencias para las que la misma evaluación y razonamiento llevarían a un resultado similar, hasta que se garantice de nuevo el cumplimiento o se ponga fin a la transferencia.

Tras dicha suspensión, la Entidad Exportadora debe poner fin a la transferencia o al conjunto de transferencias si no se puede cumplir esta Política y no se restablece el cumplimiento en el plazo de un mes desde la suspensión. En este caso, los datos personales que hayan sido transferidos antes de la suspensión, y cualquier copia de los mismos, deberán, a elección de la Entidad Exportadora, ser devueltos o destruidos en su totalidad.

El Miembro Responsable de las BCR y el DPO o Champion correspondiente, según el caso, informarán a todos los demás Miembros del Grupo de la evaluación realizada y de sus resultados, de modo que se apliquen las medidas complementarias identificadas en caso de que cualquier otro Miembro del Grupo realice el mismo tipo de transferencias o, cuando no se hayan podido aplicar medidas complementarias eficaces, se suspendan o se ponga fin a las transferencias en cuestión.

Las Entidades Exportadoras deberán hacer un seguimiento continuo y, en su caso, en colaboración con las Entidades Importadoras, de la evolución de la situación en los terceros países a los que las Entidades Exportadoras hayan transferido datos personales que pueda afectar a su evaluación inicial del nivel de protección y a las decisiones adoptadas en consecuencia sobre tales transferencias.

Regla 13B - Las Entidades Importadoras se asegurarán de que, cuando reciban una solicitud jurídicamente vinculante de una autoridad pública con arreglo a la legislación del país de destino para la divulgación de los datos personales transferidos de conformidad con la Política, o tengan conocimiento de cualquier acceso directo de las autoridades públicas a los datos personales transferidos en virtud de la Política de conformidad con la legislación del país de destino; las Entidades Importadoras lo notificarán sin demora a la Entidad Exportadora y, cuando sea posible, al interesado (si es necesario con la ayuda de la Entidad Exportadora).

Las Entidades Importadoras notificarán sin demora a la Entidad Exportadora pertinente y, en la medida de lo posible, al interesado (en caso necesario, con la ayuda de la Entidad Exportadora) cuando:

- reciban una solicitud jurídicamente vinculante, por parte de una autoridad pública en virtud de la legislación del país de destino o de otro tercer país, para la divulgación de los datos personales transferidos de conformidad con la Política (dicha notificación incluirá información sobre los datos personales solicitados, la autoridad solicitante, la base jurídica de la solicitud y la respuesta dada);

- tengan conocimiento de cualquier acceso directo por parte de las autoridades públicas a los datos personales transferidos en virtud de la Política de conformidad con la legislación del país de destino (dicha notificación incluirá toda la información de que disponga la Entidad Importadora).

Si se le prohíbe remitir tal notificación a la Entidad Exportadora y/o al interesado, la Entidad Importadora hará todo lo posible por obtener una dispensa de dicha prohibición, con vistas a comunicar a la Entidad Exportadora la mayor cantidad de información posible y lo antes posible, y documentará todas las gestiones realizadas al efecto para poder demostrarlas a petición de la Entidad Exportadora.

La Entidad Importadora proporcionará a la Entidad Exportadora, a intervalos regulares, toda la información pertinente posible sobre las solicitudes recibidas (en particular, el número de solicitudes, tipo de datos solicitados, autoridad o autoridades solicitantes, si las solicitudes han sido impugnadas y el resultado de dichas impugnaciones, etc.). Si a la Entidad Importadora se le prohíbe total o parcialmente facilitar a la Entidad Exportadora la información antes mencionada, informará de ello sin demora injustificada a la Entidad Exportadora.

La Entidad Importadora conservará la información antes mencionada mientras los datos estén sujetos a las garantías previstas en la Política y la pondrá a disposición de la autoridad de control competente a petición de ésta.

La Entidad Importadora controlará la legalidad de la solicitud de comunicación y, en particular, si la autoridad pública solicitante está debidamente facultada para ello, e impugnará la solicitud si, tras una valoración minuciosa, llega a la conclusión de que existen motivos razonables para considerar que la solicitud es ilícita con arreglo al Derecho del país de destino, incluidas las obligaciones aplicables en virtud del Derecho internacional y a los principios de cortesía internacional. La Entidad Importadora agotará, en las mismas condiciones, las vías de recurso. Al impugnar una solicitud, la Entidad Importadora instará la aplicación de medidas cautelares para suspender los efectos de la solicitud hasta que la autoridad judicial competente se haya pronunciado sobre el fondo. No comunicará los datos personales solicitados hasta que se lo exija la normativa procesal aplicable.

La Entidad Importadora documentará sus valoraciones jurídicas y las impugnaciones de solicitudes de comunicación y pondrá dicha documentación a disposición de la Entidad Exportadora en la medida en que lo permita el Derecho del país de destino. También la pondrá a disposición de la autoridad de control competente a petición de ésta.

La Entidad Importadora proporcionará la mínima información posible al responder a las solicitudes de comunicación, basándose en una interpretación razonable de la solicitud.

En cualquier caso, los Miembros del Grupo se asegurarán de que las transferencias de datos personales realizadas a cualquier autoridad pública en virtud de esta Política no sean masivas, desproporcionadas o indiscriminadas de una manera que vaya más allá de lo necesario en una sociedad democrática.

REGLA 14 - INCUMPLIMIENTO DE LA POLÍTICA Y RESCISIÓN

Regla 14A - Las Entidades Exportadoras sólo transferirán datos personales a las Entidades Importadoras que estén efectivamente vinculadas por la Política y puedan garantizar su cumplimiento.

No se efectuará ninguna transferencia en virtud de esta Política a un Miembro del Grupo a menos que dicho Miembro del Grupo esté efectivamente vinculado por la Política y pueda garantizar su cumplimiento. Cuando una Entidad Importadora no pueda cumplir la Política, por el motivo que sea, informará sin demora a la Entidad Exportadora. En caso de que la Entidad Importadora incumpla la Política o no pueda cumplirla, la Entidad Exportadora deberá suspender la transferencia.

La Entidad Importadora deberá, a elección de la Entidad Exportadora, devolver o eliminar inmediatamente los datos personales que hayan sido transferidos en virtud de la Política en su totalidad cuando:

- la Entidad Exportadora ha suspendido la transferencia y no se restablezca el cumplimiento de esta Política en un plazo razonable y, en cualquier caso, en el plazo de un mes desde la suspensión; o bien
- la Entidad Importadora incumple de forma sustancial o persistente la Política; o
- la Entidad Importadora incumple una decisión vinculante de un tribunal competente o de una autoridad de control competente en relación con sus obligaciones derivadas de la Política.

Lo mismo se aplicará a cualquier copia de los datos. La Entidad Importadora certificará la supresión de los datos a la Entidad Exportadora. Hasta que los datos sean suprimidos o devueltos, la Entidad Importadora seguirá garantizando el cumplimiento de la Política. Cuando exista una prohibición legal para que la Entidad Importadora devuelva o suprima los datos personales transferidos, la Entidad Importadora garantiza que seguirá velando por el cumplimiento de la Política y sólo tratará los datos en la medida y durante el tiempo que exija el Derecho del país.

Regla 14B - La Entidad Importadora que deje de estar vinculado por la Política garantizará que los datos personales se conservan, devuelvan o eliminen adecuadamente, según proceda.

La Entidad Importadora que deje de estar vinculada por la Política podrá conservar, devolver o eliminar los datos personales recibidos en virtud de la presente Política, según proceda. Si la Entidad Exportadora y la Importadora acuerdan que los datos pueden ser conservados por la Entidad Importadora, deberá mantenerse la protección prevista en la presente Política.

SECCIÓN C: DERECHOS DE TERCEROS BENEFICIARIOS

C.1 Los interesados cuyos datos personales se transfieran a una Entidad Importadora deben poder beneficiarse de determinados derechos como terceros beneficiarios. A tal efecto, los interesados podrán exigir el cumplimiento de:

- Reglas 1B y 1C de la Política (relativas a la licitud y lealtad, y al tratamiento de categorías especiales de datos personales);

- Regla 2 de la Política (relativa a la transparencia y al tratamiento de datos personales solo para un fin conocido);

- Regla 3 de la Política (relativa a la minimización y exactitud de los datos y a la limitación de los periodos de retención);

- Regla 4 de la Política (relativa a las medidas de seguridad apropiadas y a las obligaciones de notificación de brechas de seguridad);

- Regla 5 de la Política (relativa a garantizar los derechos de los interesados);

- Regla 6 de la Política (relativa a garantizar una protección adecuada de las transferencias y transferencias ulteriores);

- Regla 10 de la Política (relativa a la tramitación de reclamaciones);

- Regla 11 de la Política (relativa a la cooperación con las autoridades de control competentes);

- Regla 12 de la Política (relativa a la actualización de las reglas);

- Regla 13 de la Política (relativa a la actuación en caso de que la legislación nacional afecte al cumplimiento de la Política);

- Las disposiciones de C1 a C3 que conceden derechos de terceros beneficiarios y establecen las normas de responsabilidad y jurisdicción en virtud de la Política.

- Derecho a acceder a la Política disponible en la página web, en la intranet (accesible a los empleados) de la empresa o a obtener una copia impresa de la Política, así como una lista de los Miembros del Grupo vinculados por esta Política.

mediante:

- *la presentación de una reclamación*: los interesados podrán presentar reclamaciones ante un Miembro del Grupo (de conformidad con el Procedimiento de Tramitación de Reclamaciones establecido en el Apéndice 2) y ante la autoridad de control del Estado miembro en el que se haya producido la presunta infracción, o en el que el interesado trabaje o resida habitualmente; y/o

- *la interposición de acciones judiciales*: los interesados pueden interponer acciones judiciales contra los Miembros del Grupo ante los tribunales de un Estado miembro en el que el Miembro del Grupo tenga un establecimiento, o en el Estado miembro en el que el interesado tenga su residencia habitual.

Tal como se aclara en mayor detalle en las Secciones C.2 a C.4, cuando una infracción sea cometida por un Miembro del Grupo situado fuera del EEE, los interesados conservarán el derecho a presentar reclamaciones y a entablar acciones contra el Miembro Responsable de las BCR designado, como si la infracción hubiera sido cometida por dicha entidad en el Estado miembro en el que esté establecida.

Estos derechos no se extienden a los elementos de la Política relativos a los mecanismos internos aplicados entre los Miembros del Grupo, como los detalles sobre formación, el programa de auditoría, la red de cumplimiento y el mecanismo de actualización de la misma.

Asimismo, los Miembros del Grupo aceptan que los interesados puedan estar representados por una entidad, organización o asociación sin ánimo de lucro, en las condiciones establecidas en el artículo 80(1) del RGPD.

C.2 Los interesados también podrán solicitar la reparación pertinente al Miembro Responsable de las BCR, que se compromete a adoptar las medidas necesarias para remediar cualquier incumplimiento de las disposiciones enumeradas en el subapartado C.1 por parte de cualquier Entidad Importadora y, en su caso, recibir una indemnización del Miembro Responsable de las BCR por cualquier daño (material o inmaterial) sufrido como consecuencia de un incumplimiento de las disposiciones o de cualquiera de ellas enumeradas en el subapartado C.1 por parte de una Entidad Importadora de conformidad con la declaración de un tribunal u otra autoridad competente.

C.3 Para evitar cualquier tipo de duda, los interesados gozarán de los derechos de terceros beneficiarios descritos en la presente sección C, y los tribunales europeos o las autoridades de control competentes tendrán competencia como si la infracción de las disposiciones descritas en la presente sección C o de cualquiera de ellas hubiera sido causada por el Miembro Responsable de las BCR.

C.4 En caso de que se presente una reclamación en la que un interesado haya sufrido un perjuicio como consecuencia de una infracción de la presente Política, los Miembros del Grupo han acordado que la carga de la prueba para demostrar que una Entidad Importadora no es responsable de la infracción, o que dicha infracción no tuvo lugar, recaerá en el Miembro Responsable de las BCR.

PARTE III: APÉNDICES

APÉNDICE 1

PROGRAMA DE AUDITORÍA

1. INTRODUCCIÓN

1.1 Los Miembros del Grupo están obligados a auditar su cumplimiento de la Política y deben satisfacer determinadas condiciones al hacerlo. El presente documento describe la forma en que los Miembros del Grupo abordan tales requisitos.

1.2 Las funciones usuales (*business as usual* o BAU, por sus siglas en inglés) de los DPO y los Champions incluyen proporcionar directrices sobre el tratamiento de datos personales sujeto a la presente Política y evaluar el tratamiento de datos personales realizado por los Miembros del Grupo para detectar posibles riesgos relacionados con la privacidad en el día a día. Por lo tanto, el tratamiento de datos personales está sujeto a una revisión y evaluación exhaustiva y periódica.

1.3 Como 2LoD global, la Oficina Corporativa de PD asume el seguimiento y control, incluyendo la supervisión del cumplimiento de la protección de datos del Grupo Santander.

1.4 Por otro lado, el Programa de Auditoría consiste en la evaluación formal independiente realizada por la tercera línea de defensa (3LoD) para garantizar el cumplimiento de la Política, tal y como exigen las autoridades de control competentes. La opinión proporcionada por Auditoría (3LoD) es una opinión independiente y no sustituirá la necesidad de las responsabilidades de control y supervisión de 1LoD y 2LoD, que también formarán parte del alcance de la auditoría al revisar la integración y aplicación de esta Política.

2. PLANTEAMIENTO

2.1 Visión general de la auditoría

La entidad responsable de realizar las auditorías de cumplimiento de la Política y de garantizar que dichas auditorías abordan todos los aspectos de la Política puede variar en función de las circunstancias específicas de cada Miembro del Grupo. Por lo general, las auditorías son supervisadas por auditores internos o externos acreditados, según proceda (que tienen garantizada su independencia en cuanto al ejercicio de sus funciones relacionadas con estas auditorías). El auditor correspondiente será responsable de garantizar que cualquier problema o caso de incumplimiento se ponga en conocimiento de la alta dirección y que se adopten medidas correctivas para garantizar el cumplimiento en un plazo razonable.

2.2 Calendario y alcance de la auditoría

2.2.1 El departamento de Auditoría Interna determinará el calendario de las auditorías dentro un ciclo máximo de auditoría de 4 años, de conformidad con su metodología de evaluación de riesgos.

No obstante, las primeras auditorías se llevarán a cabo en los primeros 24 meses tras la aprobación formal de la Política y su consiguiente aplicación. A partir de entonces, la auditoría se realizará con arreglo a la metodología de auditoría basada en el riesgo aplicada, tal y como se indica en el primer párrafo de esta sección 2.2.

En todo caso, los Miembros del Grupo estarán obligados a llevar a cabo una auditoría cuando (i) existan indicios de incumplimiento de la presente Política; o (ii) el Equipo de Privacidad solicite una auditoría específica (ad hoc).

2.2.2 En la misma línea, el alcance y la cobertura de la auditoría serán determinados por el departamento de Auditoría Interna con arreglo a un análisis basado en el riesgo a partir de la metodología aprobada.

2.2.3 Todos los aspectos de esta Política (*e.g.,* aplicaciones, sistemas informáticos, transferencias ulteriores, etc.), incluidos los métodos y planes de acción que garanticen la aplicación de acciones correctivas, se revisarán siguiendo un enfoque basado en el riesgo para determinar el alcance específico de la auditoría y se llevarán a cabo, como se ha descrito anteriormente, a intervalos regulares adecuados.

2.3 Auditores

2.3.1 Las auditorías serán realizadas por auditores internos del departamento de Auditoría Interna o por auditores externos acreditados, según proceda. Cuando las auditorías sean realizadas por auditores externos, deberán cumplirse las siguientes condiciones:

(a) Llevar a cabo un examen de *due diligence* antes de su selección para garantizar que los auditores pertinentes tienen las cualificaciones y el estatus adecuados para ayudar en este ejercicio; y

(b) Celebrar un contrato con el mismo para regular la prestación de sus servicios de acuerdo con la normativa aplicable.

2.4 Independencia

2.4.1 Las personas encargadas de decidir sobre el programa de auditoría o de realizar las auditorías tienen garantizada la independencia en el ejercicio de sus funciones.

2.5 Informe

2.5.1 Una vez finalizada la auditoría, dependiendo de la naturaleza de la misma, el informe y las conclusiones se pondrán a disposición de los cargos de alta dirección, de la Oficina Corporativa de PD, del DPO o Champion pertinente y se informará al Comité de Auditoría del Consejo y al Consejo de Administración del Miembro Responsable de las BCR. El informe de auditoría también contendrá detalles de cualquier medida correctiva necesaria, recomendaciones y plazos para la adopción de medidas correctivas.

2.5.2 Los Miembros del Grupo acuerdan proporcionar copias de los resultados de cualquier auditoría de la Política a cualquier autoridad de control competente que lo solicite.

2.5.3 El DPO o Champion pertinente se encargará de ponerse en contacto con las autoridades de control competentes a fin de facilitar la información mencionada anteriormente.

APÉNDICE 2

PROCEDIMIENTO DE TRAMITACIÓN DE RECLAMACIONES

1. INTRODUCCIÓN

1.1 El presente procedimiento de tramitación de reclamaciones tiene por objeto explicar cómo se gestionarán las reclamaciones presentadas por un interesado cuyos datos personales sean tratados por los Miembros del Grupo en virtud de la presente Política.

2. ¿CÓMO PUEDEN RECLAMAR LOS INTERESADOS?

Todas las reclamaciones de los interesados cuyos datos personales se traten de conformidad con esta Política pueden presentarse por escrito (inclusive por correo electrónico) al DPO o Champion, según proceda. Los interesados pueden presentar una reclamación utilizando los siguientes datos de contacto:

A/A: Equipo de privacidad

Dirección: [introducir dirección postal]

Correo electrónico: Aquí encontrará una lista con las direcciones de correo electrónico pertinentes.

En todo caso, si las reclamaciones se formulan por cualquier otro medio, también serán atendidas, siempre que se notifique debidamente al Miembro del Grupo correspondiente.

3. ¿QUIÉN GESTIONA LAS RECLAMACIONES?

3.1 El DPO o Champion correspondiente, según el caso, tramitará todas las reclamaciones que surjan en virtud de la Política con respecto al tratamiento de datos personales. El DPO o Champion, según el caso, se pondrá en contacto con las unidades de negocio pertinentes para investigar la reclamación y coordinará una respuesta (que incluirá información sobre las medidas adoptadas para el reclamante).

3.2 ¿Cuál es el tiempo de respuesta?

El DPO o Champion, con el apoyo del Equipo de Privacidad, acusará recibo de la reclamación al interesado en el plazo de diez días laborables, investigará y posteriormente dará una respuesta sustantiva facilitando información sobre las medidas adoptadas sin dilación indebida y, en cualquier caso, en el plazo de un mes natural. Si, debido a la complejidad de la reclamación o al número de solicitudes, no puede darse una respuesta sustantiva en este plazo, el DPO o Champion, con el apoyo del Equipo de Privacidad, informará al reclamante de los motivos del retraso en el plazo de un mes natural a partir de la recepción de la reclamación, y facilitará un plazo estimado razonable (que no exceda de otros dos meses naturales a partir de la fecha en que se notificó la ampliación al interesado) para la respuesta.

Si no se cumple el plazo de respuesta y la respuesta a la reclamación se retrasa sin motivo justificado, el interesado puede notificar este hecho al DPO o al Champion, quienes, sin dilación indebida y en cualquier caso en el plazo de diez días naturales, explicarán los motivos de dicho retraso e informarán al interesado de las medidas adoptadas hasta el momento. El asunto se remitirá a la Oficina

Corporativa de PD (junto con un informe motivado en el que se determinen las medidas a adoptar), que revisará el caso y asesorará al DPO o Champion sobre cómo resolver las cuestiones objeto de la reclamación a la mayor brevedad posible. En cualquier caso, el interesado también podrá hacer uso de los derechos descritos en el apartado 3.4 del presente Apéndice 2.

3.3 Cuando un reclamante impugne una decisión o la desestimación de una reclamación

Si una reclamación se considera justificada, el DPO o Champion tomarán las medidas necesarias para resolver la cuestión planteada por el interesado y le informarán al respecto.

Si el reclamante discrepa con la respuesta del DPO o Champion (inclusive si dicha respuesta es una negativa a atender / satisfacer la reclamación) o con cualquier decisión, puede notificarlo al DPO o Champion pertinente. El asunto se remitirá a la Oficina Corporativa de PD, que revisará el caso para que, a través del DPO o Champion de la entidad, se comunique al reclamante la decisión final de aceptar la decisión original o de sustituirla por una nueva. La Oficina Local de PD correspondiente responderá al reclamante en el plazo de un mes natural a partir de la remisión. Si, debido a la complejidad de la reclamación, no puede darse una respuesta sustantiva en este plazo, la Oficina Corporativa de PD comunicará al reclamante el motivo del retraso en el plazo de un mes natural a partir de la recepción de la remisión, y facilitará un estimación de plazo razonable para la respuesta (que no excederá de otros dos meses naturales). Si la reclamación es admitida a trámite, la Oficina Corporativa de PD dispondrá que se tomen las medidas necesarias en consecuencia.

3.4 Mecanismos alternativos de reclamación

Los interesados cuyos datos personales se traten de conformidad con esta Política también tienen derecho a: (i) presentar una reclamación ante la autoridad de control competente del Estado miembro en el que se haya producido la presunta infracción, o en el que trabaje o resida habitualmente el interesado; y/o (ii) acudir ante un tribunal competente del país europeo en el que esté establecido el Miembro del Grupo o del país europeo en el que resida el interesado. Tal como se aclara en mayor detalle en las Secciones C.2 a C.4, cuando una infracción sea cometida por un Miembro del Grupo situado fuera del EEE, los interesados conservarán el derecho a presentar reclamaciones y a entablar acciones contra el Miembro Responsable de las BCR designado, como si la infracción hubiera sido cometida por dicha entidad en el Estado miembro en el que esté establecida. Estos derechos se aplicarán con independencia de que el interesado haya presentado primero una reclamación a un Miembro del Grupo a través de este Procedimiento de Tramitación de Reclamaciones.

APÉNDICE 3

PROCEDIMIENTO DE COOPERACIÓN

1. PROCEDIMIENTO DE COOPERACIÓN

1.1 El presente Procedimiento de Cooperación establece la forma en que los Miembros del Grupo cooperarán con las autoridades de control competentes y aceptarán ser auditados e inspeccionados por ellas (incluso, cuando sea necesario, *in situ*) en relación con esta Política; así como tener en cuenta sus consejos y acatar sus decisiones sobre cualquier asunto relacionado con esta Política.

1.2 Cuando sea necesario, los Miembros del Grupo pondrán a su disposición el personal adecuado para dialogar con la autoridad de control competente en relación con la Política.

1.3 Previa solicitud, el DPO o Champion pertinente o el departamento de Auditoría Interna, según proceda, proporcionará copias de los resultados de cualquier auditoría de la Política conforme al Apéndice 1, así como cualquier información sobre las operaciones de tratamiento cubiertas por la Política a cualquier autoridad de control competente, a la que se recordará al recibir dicha información su deber de secreto profesional.

1.4 Los Miembros del Grupo aceptan que las autoridades de control competentes puedan llevar a cabo una auditoría de protección de datos o una inspección (incluso, en caso necesario, *in situ*) de ellos mismos de conformidad con la Normativa Europea de Protección de Datos de la Entidad Exportadora pertinente.

1.5 Todos los Miembros del Grupo aceptan ser auditados por las autoridades de control competentes de conformidad con los procedimientos de auditoría aplicables de dichas autoridades de control.

1.6 Los Miembros del Grupo acuerdan que cualquier litigio relacionado con el ejercicio de los poderes de supervisión de una autoridad de control competente sobre esta Política será resuelto por los tribunales del Estado miembro en el que se encuentre dicha autoridad de control, de conformidad con la legislación procesal de dicho Estado miembro.

APÉNDICE 4

PROCEDIMIENTO DE ACTUALIZACIÓN

1. INTRODUCCIÓN Y PRINCIPIOS GENERALES

1.1 Este Procedimiento de Actualización establece la forma en que se comunicarán los cambios de la Política a las autoridades de control competentes, a los interesados y a los Miembros del Grupo vinculados por la Política

1.2 La Política se mantendrá actualizada para reflejar la situación y el entorno actuales en materia de protección de datos personales.

2. MODIFICACIONES SUSTANCIALES DE LA POLÍTICA

2.1 El DPO de Banco Santander y Asesoría Jurídica Corporativa, comunicarán con antelación cualquier cambio material en la Política (es decir, cualquier modificación que pudiera ir en detrimento del nivel de protección ofrecido por la Política o afectar de manera significativa a la Política -e.g., cambios en su carácter vinculante-) a la Agencia Española de Protección de Datos (la "**Autoridad de Control Principal de las BCR**") y, a través de la Autoridad de Control Principal de las BCR, a las autoridades de control. Dicha comunicación incluirá una breve explicación de los motivos de la actualización. La autoridad de control pertinente también evaluará si los cambios introducidos requieren una nueva aprobación.

3. OTRAS MODIFICACIONES DE LA POLÍTICA

3.1 El DPO del Banco Santander y Asesoría Jurídica Corporativa, comunicarán a la Autoridad de Control Principal de las BCR (y a través de éste a las otras autoridades de control implicadas) cuando se le solicite, y al menos una vez al año, los cambios en la Política (o la ausencia de los mismos). Esta actualización anual también incluirá la renovación de la confirmación relativa a que el Miembro Responsable de las BCR tiene activos suficientes, o ha tomado las medidas adecuadas para poder pagar una indemnización por daños y perjuicios derivados de un incumplimiento de la Política.

3.2 Entre los ejemplos de los cambios mencionados pueden incluirse los de naturaleza administrativa (incluidas las actualizaciones de la lista de Miembros del Grupo); los que se hayan producido como resultado de un cambio de la Normativa Europea de Protección de Datos aplicable; o los derivados de cualquier medida y directriz legislativa, decisión judicial o de las autoridades de control (incluidas las directrices del Comité Europeo de Protección de Datos). Banco Santander también proporcionará una breve explicación a la Autoridad de Control Principal de las BCR y a las otras autoridades de control sobre los motivos de cualquier cambio notificado en la Política.

4. NUEVOS MIEMBROS DEL GRUPO

4.1 Los DPO y los Champion (junto con el Equipo de Privacidad) se asegurarán de que todos los nuevos Miembros del Grupo estén efectivamente vinculados por la Política y puedan cumplirla antes de llevar a cabo una transferencia de datos personales a los Miembros del Grupo.

5. COMUNICACIÓN Y REGISTRO DE LOS CAMBIOS INTRODUCIDOS EN LA POLÍTICA

5.1 La Política contiene un registro de cambios que establece la fecha de las modificaciones de la Política y los datos de cualquier modificación realizada. Asesoría Jurídica Corporativa mantendrá una lista actualizada de los cambios realizados en la Política y la Oficina Corporativa de PD mantendrá la lista de los Miembros del Grupo vinculados a la misma.

5.2 Asesoría Jurídica Corporativa, con el apoyo de la Oficina Corporativa de PD, comunicará todos los cambios que se introduzcan en la Política, ya sean de naturaleza material o de otro tipo:

(a) a los Miembros del Grupo vinculados por la Política, sin dilaciones indebidas, y publicará una versión actualizada de esta Política en la intranet del Grupo Santander;

(b) sistemáticamente a los interesados que se beneficien de la Política, a través de la página web de la empresa (Web Corporativa Santander); y

(c) bajo petición y a través de los DPO (o figura similar) locales, a la autoridad de control competente.