GRUPPO SANTANDER

NORME VINCOLANTI D'IMPRESA (BCR) PER I TITOLARI DEL TRATTAMENTO

INDICE PAGINA

INTRODUZIONE

Le presenti norme vincolanti d'impresa (BCR, dall'inglese Binding Corporate Rules) per i titolari del trattamento e le relative appendici (in prosieguo, congiuntamente, le "**Norme**") descrivono l'approccio di Banco Santander, S.A. ("**Banco Santander**") in materia di protezione e gestione dei dati personali da parte dei membri del Gruppo Santander, come di seguito definito, che hanno aderito alle presenti Norme, nel contesto dei trasferimenti internazionali di tali dati personali tra i Membri del Gruppo, come definiti di seguito.

Banco Santander è la società capogruppo nonché la sede centrale di uno dei maggiori gruppi finanziari in Spagna, composto da controllate sia spagnole che estere ("**Gruppo Santander**"), dedicato principalmente alla fornitura di servizi finanziari globali a livello mondiale nei seguenti ambiti: (i) **Retail & Commercial Banking**: comprende tutte le attività di retail e commercial banking di Santander; (ii) **Corporate & Investment Banking**: supporta i clienti corporate e istituzionali attraverso servizi su misura e prodotti all'ingrosso a valore aggiunto tramite le divisioni Markets, Investment Banking (Global Debt Finance e Corporate Finance) e Global Transactional Banking; (iii) **Wealth Management & Insurance:** riunisce le attività di private banking, asset management e assicurative attraverso Santander Private Banking, Santander Asset Management e Santander Insurance; (iv) **Digital Consumer Bank**: riunisce la piattaforma digitale Openbank e Santander Consumer Finance, creando un modello unico nei diversi mercati per le attività di credito al consumo e finanziamento auto; e (v) **PagoNxt & Cards**: comprende PagoNxt, che riunisce tutte le attività di pagamento di Santander, e Global Cards, l'attività e la piattaforma di Santander dedicata alle carte, offrendo opzioni di pagamento digitali e soluzioni tecnologiche globali per le banche di Santander e i nuovi clienti. Oltre a quanto sopra, il Gruppo Santander comprende anche la **Centrale e altre funzioni che prestano servizi all'intero Gruppo**, ossia le aree incaricate di fornire supporto e assistere tutti i Membri del Gruppo nello svolgimento di tutti i compiti necessari a livello di Gruppo e non strettamente connessi alla loro attività principale (ad es., gestione del personale, adempimento degli obblighi di legge, audit, gestione dei rischi, ecc.).

Oltre alle altre definizioni contenute nelle presenti Norme, si applicano le seguenti definizioni:

"**normativa locale applicabile in materia di protezione dei dati**": qualsiasi legge nazionale o locale in materia di protezione dei dati (inclusa, se del caso, la normativa europea sulla protezione dei dati) applicabile ai Membri del Gruppo, purché rispetti l'essenza dei diritti e delle libertà fondamentali e non ecceda quanto necessario e proporzionato in una società democratica, in linea con i requisiti di cui alla Norma 13;

"**autorità di controllo competente**": l'autorità di controllo del SEE competente per l'Esportatore;

"**titolare del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

"**Europa**" o "**SEE"**: i Paesi dello Spazio economico europeo;

"**normativa europea sulla protezione dei dati personali**": il GDPR e qualsiasi legge in materia di protezione dei dati di uno Stato membro europeo, ivi compresa la legislazione locale di attuazione dei requisiti del GDPR e la normativa derivata, nella versione vigente;

"**Esportatore**": un Membro del Gruppo stabilito in Europa, o comunque soggetto alla normativa europea sulla protezione dei dati personali, che trasferisce, o mette altrimenti a disposizione, dati personali a un Importatore ai sensi delle presenti Norme;

"**GDPR**": il Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati);

"**Membro/i del Gruppo**": i membri del Gruppo Santander che hanno aderito alle presenti Norme;

"**Importatore**": un Membro del Gruppo stabilito al di fuori dell'Europa che riceve dati personali da un Esportatore e tratta i dati personali trasferiti al di fuori del SEE;

"**Membro responsabile per le violazioni (delle norme vincolanti d'impresa)**": Banco Santander (ovvero, Banco Santander S.A. come sopra definito);

"**dato personale**": qualsiasi informazione relativa a una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on-line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

"**trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

"**responsabile del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

"**profilazione**": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

"**categorie particolari di dati personali**" o "**dati sensibili**": i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici trattati al fine di identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona fisica; e

"**autorità di controllo**": un'autorità pubblica indipendente istituita da uno Stato membro in una giurisdizione europea, che è responsabile della vigilanza sull'applicazione della normativa europea sulla protezione dei dati personali al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche in relazione al trattamento e di agevolare la libera circolazione dei dati personali all'interno del SEE.

Le presenti Norme si applicano a tutti i dati personali soggetti alla normativa europea sulla protezione dei dati che gli Esportatori trasferiscono agli Importatori. Si applicano inoltre agli eventuali trasferimenti successivi effettuati dagli Importatori verso altri Importatori o terzi situati al di fuori del SEE, nel rispetto dei requisiti previsti dalla Norma 6. Pertanto, eventuali obblighi e requisiti assegnati ai Membri del Gruppo ai sensi delle presenti Norme saranno applicabili nella misura in cui si riferiscono ai dati personali che rientrano in tale ambito di applicazione.

Le presenti Norme si applicano a tutti tali dati personali trattati dai Membri del Gruppo come descritto nelle sezioni "*Quali dati personali sono disciplinati dalle presenti Norme?*" e "*Per quali finalità vengono trasferiti i dati personali ai sensi delle presenti Norme?*".

I Membri del Gruppo e i loro dipendenti sono tenuti a osservare e rispettare pienamente le presenti Norme nel trattamento dei dati personali disciplinato dalle stesse.

Le presenti Norme integrano, senza sostituire né prevalere su di essi, eventuali requisiti o norme specifici in materia di riservatezza o segreto applicabili a un'area aziendale o a una funzione del Gruppo Santander o previsti dalla normativa applicabile, purché tale normativa sia conforme ai requisiti di cui alla Norma 13.

Le presenti Norme, unitamente all'elenco degli attuali Membri del Gruppo e ai rispettivi recapiti indicati nell'Appendice 5, sono pubblicate sul sito web aziendale, accessibile al pubblico **qui.**

Applicazione ai trasferimenti effettuati da Membri del Gruppo non soggetti alla normativa europea sulla protezione dei dati

Qualora un Membro del Gruppo non soggetto alla normativa europea sulla protezione dei dati sia oggetto di restrizioni sui trasferimenti internazionali di dati personali ai sensi della normativa locale applicabile in materia di protezione dei dati e le autorità locali del relativo Paese riconoscono (integralmente o parzialmente, secondo quanto previsto da tale normativa locale) le presenti Norme quale meccanismo valido per legittimare i trasferimenti internazionali di dati personali, le presenti Norme si possono applicare anche ai dati personali trasferiti da tali Paesi agli Importatori. A scanso di equivoci, ciò non pregiudica l'applicazione al Membro del Gruppo situato al di fuori dell'Europa della normativa locale applicabile in materia di protezione dei dati.

In tali casi, le definizioni di cui sopra devono essere interpretate considerando quale Esportatore il Membro del Gruppo che trasferisce dati personali non soggetti alla normativa europea sulla protezione dei dati. Di conseguenza, le presenti Norme vanno interpretate e applicate *mutatis mutandis* (ad esempio, la normativa europea sulla protezione dei dati deve essere interpretata come la normativa locale applicabile in materia di protezione dei dati, l'autorità di controllo competente come l'autorità locale competente nella giurisdizione pertinente e lo Stato membro come il Paese interessato).

In tale contesto, il Membro del Gruppo che trasferisce dati personali non soggetto alla normativa europea sulla protezione dei dati agirà in qualità di Membro responsabile per le violazioni in relazione a tali trasferimenti internazionali di dati.

PARTE I: CONTESTO E AZIONI

CHE COS'È LA NORMATIVA EUROPEA SULLA PROTEZIONE DEI DATI?

La normativa europea sulla protezione dei dati conferisce alle persone il diritto di controllare in che modo vengono trattati i loro dati personali. Ai sensi della normativa europea sulla protezione dei dati, quando un'organizzazione tratta dati personali per le proprie finalità è considerata il titolare del trattamento di tali informazioni ed è pertanto la principale responsabile del rispetto dei requisiti legali. Ad esempio, un datore di lavoro è il titolare del trattamento dei dati personali relativi ai propri dipendenti.

Quando, invece, un'organizzazione tratta informazioni per conto di un altro soggetto (ad esempio, per fornire un servizio) è considerata la responsabile del trattamento dei dati.

IN CHE MODO LA NORMATIVA EUROPEA SULLA PROTEZIONE DEI DATI INCIDE SUI TRASFERIMENTI DI DATI PERSONALI TRA I MEMBRI DEL GRUPPO?

La normativa europea sulla protezione dei dati non consente i trasferimenti di dati personali verso Paesi, territori od organizzazioni internazionali al di fuori dell'Europa che non garantiscano un livello adeguato di tutela dei diritti delle persone fisiche in materia di protezione dei dati. Poiché alcuni dei Paesi in cui operano i Membri del Gruppo non sono ritenuti dalla Commissione europea in grado di garantire un livello di protezione adeguato, devono essere adottate garanzie idonee per soddisfare i requisiti della normativa europea sulla protezione dei dati.

COSA STANNO FACENDO I MEMBRI DEL GRUPPO AL RIGUARDO?

I Membri del Gruppo devono adottare misure adeguate per garantire che il trattamento dei dati personali, durante i trasferimenti a livello internazionale, sia sicuro e lecito. Lo scopo delle presenti Norme, pertanto, è definire un quadro volto a soddisfare gli standard contenuti nella normativa europea sulla protezione dei dati e, di conseguenza, garantire un livello adeguato di protezione di tutti i dati personali trasferiti dagli Esportatori agli Importatori.

Le presenti Norme sono giuridicamente vincolanti e si applicano a tutti i Membri del Gruppo e ai loro dipendenti qualora tali Membri del Gruppo trattino dati personali, sia manualmente che con strumenti automatizzati. Le presenti Norme impongono ai Membri del Gruppo di rispettare le Norme riportate nella Parte II, ove applicabili, nonché le politiche e le procedure indicate nelle Appendici della Parte III. Se un Importatore è soggetto a una normativa locale applicabile in materia di protezione dei dati riconosciuta come in grado di garantire un livello di protezione adeguato ai sensi della normativa locale applicabile in materia di protezione dei dati dell'Esportatore e offre un livello di protezione equivalente a quello previsto dalle presenti Norme, i processi e le procedure locali sostanzialmente conformi ai requisiti delle presenti Norme saranno considerati validi, anche qualora introducano variazioni o differenze procedurali (ad es., team locali che gestiscono determinate procedure), purché tali variazioni siano coerenti con le presenti Norme. I trasferimenti internazionali disciplinati dalle presenti Norme comprendono i trasferimenti di dati personali dai Membri del Gruppo che rientrano nell'ambito di applicazione territoriale del GDPR ai sensi dell'articolo 3 dello stesso ai Membri del Gruppo situati al di fuori del SEE, nonché i successivi trasferimenti da questi ultimi ad altri Membri del Gruppo o a terzi esterni al di fuori del SEE, nel rispetto dei requisiti di cui alla Norma 6 che segue.

COSA SUCCEDE AI MEMBRI DEL GRUPPO NON SOGGETTI ALLA NORMATIVA EUROPEA SULLA PROTEZIONE DEI DATI CHE ESPORTANO DATI?

Come spiegato nell'introduzione e al fine di predisporre un quadro globale di protezione dei dati per il Gruppo Santander, qualora un Membro del Gruppo non soggetto alla normativa europea sulla protezione dei dati sia

oggetto di restrizioni sui trasferimenti internazionali di dati personali ai sensi della propria normativa locale applicabile in materia di protezione dei dati e le autorità locali dei Paesi in questione riconoscano (integralmente o parzialmente, come richiesto dalla normativa locale applicabile in materia di protezione dei dati) le presenti Norme quale meccanismo valido per legittimare i trasferimenti internazionali di dati personali, le presenti Norme potranno applicarsi anche ai dati personali trasferiti da tali Paesi agli Importatori. A scanso di equivoci, ciò non pregiudica l'applicazione al Membro del Gruppo situato al di fuori dell'Europa della normativa locale applicabile in materia di protezione dei dati.

QUALI DATI PERSONALI SONO DISCIPLINATI DALLE PRESENTI NORME?

Le presenti Norme disciplinano il trattamento dei seguenti dati personali:

- Per quanto concerne i dati personali dei **dipendenti ed ex dipendenti e di altro personale (quali tirocinanti, lavoratori distaccati o collaboratori autonomi)**:

  (a) Dati personali e di contatto (ad es., nome, secondo nome, cognome, titolo, alias, firma, sesso, data di nascita, cittadinanza, numeri/documenti di identificazione nazionale, indirizzo e-mail, indirizzo di residenza, numeri di telefono, fotografia, permessi di lavoro, ecc.); **(b) Dati relativi al rapporto di lavoro, compresi il percorso professionale, le condizioni di lavoro e i dati di contatto** (ad es., e-mail e numero di telefono aziendali, numero identificativo del dipendente, nome utente/codice di accesso assegnato (utilizzato, ad es., per accedere al terminale della postazione di lavoro), percorso professionale, posizione attuale, ruolo, mansioni, società, sede di lavoro, unità operativa, numero identificativo del dipartimento, numero identificativo della filiale, Paese in cui viene svolta l'attività, identificativo e nome del/dei superiore/i e del/dei sottoposto/i, stato e tipologia del rapporto di lavoro, eventuale qualifica di lavoratore esterno, data di assunzione, data di inizio dell'incarico e, se del caso, data di cessazione, dati contrattuali, piani pensionistici, flessibilità lavorativa, richieste di mobilità, dotazione, dati relativi alla conformità alle politiche interne o ad altre disposizioni di legge applicabili, valutazioni e giudizi sulle prestazioni, compresi i riscontri di responsabili, parti interessate e altre persone che lavorano con il dipendente, promozioni e provvedimenti disciplinari, ecc.); **(c) Dati relativi a talento, selezione e candidatura, istruzione e formazione** (*ad* es., dati contenuti nelle lettere di candidatura e nei résumé o CV, dati su piano di sviluppo e valutazione, dati sulla formazione, sito web personale o profilo LinkedIn forniti direttamente dai dipendenti, esperienze lavorative precedenti e referenze, percorso di formazione, qualifiche professionali, competenze linguistiche e altre competenze pertinenti, ecc.); **(d) Informazioni finanziarie, compresi i dati relativi alla retribuzione e alle paghe** (ad es., coordinate bancarie, stipendio, piani a benefici definiti, bonus, valuta, retribuzione variabile, dati relativi a piani di stock option e stock grant e altri incentivi, frequenza dei pagamenti, data di decorrenza della retribuzione attuale, revisioni salariali, codice fiscale, ecc.); **(e) Dati relativi alla sicurezza e ai sistemi informatici** (ad es., ID utente, chiave di accesso agli strumenti, credenziali di accesso, credenziali e profili di sicurezza, e-mail inviate e ricevute mediante gli account di posta elettronica aziendali, nei limiti consentiti dalla legge, informazioni acquisite attraverso l'utilizzo dei sistemi informatici, comprese le informazioni relative all'accesso e all'autenticazione, cronologia di navigazione in Internet, numeri telefonici chiamati, documenti e file archiviati nei sistemi o nelle reti aziendali, compresi i desktop dei computer, registri, indirizzo IP, tentativi di accesso riusciti e non riusciti, informazioni raccolte mediante cookie o altre tecnologie di tracciamento analoghe, ecc.); (f) **Dati relativi all'orario di lavoro** (ad es., ferie, giorni e periodi di assenza, altri congedi e relativa documentazione giustificativa, se del caso, date di rientro dopo i congedi, altri dati relativi alle assenze, registrazione delle ore lavorate, ove prevista o consentita dalla legge, lavoro straordinario, turno di lavoro, ecc.); e **(g) Qualsiasi altra informazione fornita volontariamente dagli interessati** (ad es., mediante indagini sul coinvolgimento del personale o altri sondaggi, ecc.).

Inoltre, **categorie particolari di dati personali** (**nello specifico, ma non solo, dati relativi alla salute e all'appartenenza sindacale**) possono essere trattate dai Membri del Gruppo quando necessario e richiesto o consentito dalla legge applicabile per le finalità descritte nella sezione seguente.

- Per quanto concerne i dati personali **dei familiari dei dipendenti**:

  (a) Dati anagrafici e di contatto (ad esempio, nome, cognome, sesso, numeri/documenti di identificazione nazionale, dati di contatto quali il numero da contattare in caso di emergenza, ecc.); e **(b) Altre informazioni relative ai dipendenti o alla rispettiva famiglia, ove richiesto/consentito dalla legge** (ad esempio, nucleo e situazione familiare, rapporto di parentela con il dipendente, nome e altre informazioni pertinenti su figli e altri soggetti a carico, stato civile, dati relativi alla conformità alle politiche interne o ad altre disposizioni di legge applicabili, ecc.).

- Per quanto concerne i dati personali **dei candidati attuali ed ex candidati**:

  (a) Dati personali e di contatto (ad esempio, nome, cognome, Paese, Stato e città di residenza, indirizzo e-mail, indirizzo di residenza, numeri di telefono, cittadinanza, ecc.); **(b) Dati relativi a selezione, istruzione e formazione** (ad esempio, dati contenuti nelle lettere di candidatura e nel résumé/CV, sito web personale o profilo LinkedIn forniti direttamente dai candidati, esperienze lavorative precedenti e referenze, percorso di istruzione, qualifiche professionali, competenze linguistiche e altre competenze pertinenti, informazioni sulle valutazioni della gestione delle prestazioni, piano di sviluppo e disponibilità al trasferimento, dati personali derivati dalla partecipazione dei candidati al processo di selezione (ad esempio, ottenuti durante i colloqui individuali e le e-mail scambiate in merito alle candidature o alle conversazioni intercorse), ecc.); e **(c) Informazioni audio e visive** (ad esempio, voce e immagine acquisite mediante fotografie, registrazioni video o audio nel contesto di colloqui condotti telefonicamente o in videoconferenza, ecc.).

- Per quanto concerne i dati personali dei **clienti potenziali e attuali** (compresi quelli dei loro eventuali dipendenti, rappresentanti e/o agenti, nonché utenti autorizzati e utenti del sito web):

  (a) Dati personali e di contatto *(*ad es., nome, secondo nome, cognome, numero di telefono, indirizzo e-mail, indirizzo postale, Paese di residenza, regione, cittadinanza o nazionalità, numeri/documenti di identificazione nazionale, sesso, lingua, data di nascita, Paese di nascita, stato civile, dati relativi alla situazione familiare o sociale, quali il numero di persone a carico, eventuale minore età dell'interessato o necessità di un rappresentante legale, dati demografici e socioeconomici, ecc.); **(b) Dati professionali** (ad es., professione, posizione, percorso professionale e formativo, dati relativi alla società, recapiti professionali, occupazione, categoria e qualifica professionale, ecc.); **(c) Dati (pre)contrattuali** (ad es., codice della categoria, capacità giuridica, dati relativi alle procure, numero di registrazione e indicatore interno del cliente, livello di relazione, rapporto commerciale con Santander, prodotti o servizi sottoscritti o richiesti, valutazione del rischio (risk scoring), informazioni provenienti da sistemi di informazioni creditizie, ordini di acquisto, dati statistici, fatture, informazioni su beni e attività patrimoniali, sovvenzioni, informazioni sui conti e sulle operazioni, nella misura consentita dalla normativa applicabile, contratti e altri accordi che possono contenere dati personali relativi agli interessati in questione e alla relativa esecuzione, ecc.); **(d) Informazioni finanziarie, fiscali e di pagamento** (ad es., coordinate bancarie, dati dei beneficiari, saldi attuali e storici dei prodotti e servizi e cronologia dei pagamenti, dati delle carte di credito, accredito diretto dello stipendio, dati/tipologia del reddito, fondi disponibili, operazioni monetarie, importo dei pagamenti, dati delle rimesse, dati sulla solvibilità, numero di identificazione fiscale, Paese di residenza fiscale, saldo fiscale annuale, ecc.); **(e) Dati relativi alla conformità** (ad es., identificativo della persona politicamente esposta collegata, rapporto ai sensi della MiFID o rapporto analogo (ad es., rapporti associativi o legami familiari), tipologia di rapporto (ad es., coniuge, parente, azionista o rappresentante legale, ecc.), data di inizio e, se del caso, di cessazione del rapporto, informazioni relative agli obblighi in materia di antiriciclaggio e prevenzione

delle frodi, quali profili, informazioni e valutazioni contenute nelle banche dati sulla solvibilità e sui rischi, ecc.); **(f) Informazioni audio e visive** (ad es., voce e immagine acquisite mediante fotografie o registrazioni video o audio nell'ambito di riunioni svolte telefonicamente o in videoconferenza oppure per finalità di sicurezza, ecc.); **(g) Informazioni informatiche** (ad es., indirizzo IP, ID utente, password, registri, compresi i dati del profilo, relativi ai siti web o ai portali del Gruppo Santander, chiavi di accesso agli strumenti, credenziali e profili di sicurezza, dati di autenticazione informatica, cronologia di navigazione, ID del dispositivo, identificativo pubblicitario, social network, ecc.); e **(h) Altri dati relativi al rapporto professionale con il Gruppo Santander** (ad es., dati relativi ai reclami, comunicazioni condivise, preferenze in materia di comunicazioni, richieste, ecc.).

Inoltre, i Membri del Gruppo possono trattare **categorie particolari di dati personali (compresi i dati personali relativi a condanne penali e reati, nel contesto della gestione dei rischi e delle sanzioni internazionali)**, ove ciò sia necessario e richiesto o consentito dalla normativa applicabile, per le finalità descritte nella sezione seguente.

- Per quanto concerne i dati personali dei **fornitori, venditori o prestatori di servizi attuali e potenziali** (compresi quelli dei loro eventuali dipendenti, rappresentanti e/o agenti):

  (a) Dati personali, professionali e di contatto (ad es., nome, cognome, numero di telefono, indirizzo e-mail, indirizzo postale, numeri/documenti di identificazione nazionale, posizione/qualifica professionale, dati della società, recapiti professionali, ecc.); **(b) Dati contrattuali** (ad es., dati relativi alle procure, ordini di acquisto, fatture, contratti e altri accordi che possono contenere dati personali relativi agli interessati in questione, ecc.); **(c) Informazioni finanziarie e di pagamento** (ad es., coordinate bancarie, dati delle carte di credito, dati sulla solvibilità, ecc.); **(d) Informazioni audio e visive** (ad es., voce e immagine acquisite mediante fotografie o registrazioni video o audio nell'ambito di riunioni svolte telefonicamente o in videoconferenza oppure per finalità di sicurezza, comprese le informazioni acquisite mediante sistemi di controllo degli accessi e telecamere di sicurezza, ecc.); **(e) Informazioni informatiche** (ad es., indirizzo IP, ID utente, password, registri, compresi i dati del profilo, relativi ai siti web o ai portali del Gruppo Santander, ecc.); e **(f) Altri dati relativi al rapporto professionale con il Gruppo Santander** (ad es., dati relativi ai reclami, comunicazioni condivise, ecc.).

- Per quanto concerne i dati personali degli **azionisti**:

  (a) Dati personali, professionali e di contatto (ad es., nome, cognome, sesso, data di nascita, numero di telefono, indirizzo e-mail, indirizzo postale, numeri/documenti di identificazione nazionale, posizione/qualifica professionale, dati relativi alla società, recapiti professionali, numero dell'azionista, nazionalità/cittadinanza, Paese di nascita e di residenza, ecc.); **(b) Informazioni finanziarie e di pagamento** (ad es., coordinate bancarie, dati delle carte di credito, dati relativi ai pagamenti, numero di azioni, documenti relativi alla proprietà e ai dividendi, operazioni monetarie, movimenti, posizioni e titolari di azioni di altre società, informazioni sui prodotti finanziari sottoscritti, ecc.); e **(c) Informazioni informatiche** (ad es., indirizzo IP, ID utente, password, registri, compresi i dati del profilo, relativi ai siti web o ai portali del Gruppo Santander, ecc.).

- Per quanto riguarda i dati personali degli **utenti web, degli utenti finali e degli utenti istituzionali (compresi quelli di piattaforme/siti web/app relativi al mondo universitario, al lavoro e all'imprenditorialità):**

  (a) **Dati personali e di contatto** (ad es., nome, cognome, data di nascita, sesso, indirizzo e-mail, indirizzo postale, numeri di telefono, Paese di residenza, nazionalità, numeri di identificazione nazionale, ecc.); **(b) Dati professionali e relativi all'istruzione** (ad es., posizione/qualifica professionale, dati relativi alla società, recapiti professionali, percorso professionale, CV, dati accademici, istruzione o qualifiche, dati demografici e socioeconomici, legami con progetti imprenditoriali o società, ecc.); **(c) Informazioni**

informatiche (ad es., indirizzo IP, ID utente, password, registri relativi all'utilizzo, compresi i dati del profilo, di siti web o portali, registrazioni delle chiamate, ecc.); **(d) Dati di navigazione e di utilizzo** (ad es., informazioni raccolte automaticamente dagli interessati, mediante cookie o altre tecnologie analoghe, riguardanti l'utilizzo di siti web/dispositivi, compresi i profili, la navigazione web, i dati di utilizzo, ecc.); e **(e) Altri dati relativi al rapporto con il Gruppo Santander** (ad es., richieste di informazioni, interessi, comunicazioni condivise, ecc.).

PER QUALI FINALITÀ VENGONO TRASFERITI I DATI PERSONALI AI SENSI DELLE PRESENTI NORME?

I dati personali vengono trasferiti tra i Membri del Gruppo in tutto il mondo (principalmente in Argentina, Bahamas, Brasile, Colombia, Paesi europei, Messico, Perù, Svizzera, Regno Unito, Stati Uniti d'America, Uruguay, ecc.) ai sensi delle presenti Norme, per le seguenti finalità ed esclusivamente nei limiti consentiti dalla normativa applicabile:

- I dati personali dei **dipendenti ed ex dipendenti e di altro personale (quali tirocinanti, lavoratori distaccati o collaboratori autonomi)** vengono trasferiti per le seguenti finalità: **(a) amministrazione e gestione del personale** (ad es., gestione, pianificazione e monitoraggio della formazione, gestione delle prestazioni, gestione delle paghe e dei benefit, promozioni, pianificazione delle successioni e sviluppo professionale, gestione della mobilità interna, dei trasferimenti e dei distacchi, compilazione e gestione degli elenchi dei dipendenti esistenti, organizzazione delle trasferte di lavoro, gestione delle spese professionali e dei relativi rimborsi, agevolazione delle comunicazioni aziendali, delle trattative, delle operazioni e delle conferenze, verifica dell'adempimento degli obblighi e dei doveri lavorativi dei dipendenti, gestione dei congedi e delle assenze, valutazioni del personale, gestione e segnalazione di questioni disciplinari e cessazioni dei rapporti di lavoro, riesame delle decisioni in materia di lavoro, accertamento dell'idoneità al lavoro dei dipendenti e adozione delle relative decisioni, nonché degli adeguamenti delle postazioni di lavoro, monitoraggio del rispetto delle politiche e delle procedure interne e altre attività di controllo previste dalla normativa applicabile, quali i sistemi interni di segnalazione, compreso il rispetto del Codice di condotta sui mercati mobiliari o di politiche analoghe e dei relativi obblighi, tra cui l'approvazione e il monitoraggio delle operazioni su conti personali, analisi e pianificazione della forza lavoro, svolgimento di verifiche dei precedenti personali ove previsto o consentito dalla normativa applicabile, ecc.); **(b) svolgimento in forma aggregata di segmentazioni, statistiche e analisi** relative ai dati sull'attività dei dipendenti, al fine di comprendere meglio la popolazione aziendale e orientare le decisioni che la riguardano, tra l'altro in materia di ricerca dei talenti, pianificazione professionale e pianificazione delle successioni; **(c) supporto alla gestione dei servizi forniti dal Gruppo Santander e delle sue attività operative** (ad es., gestione e protezione dei sistemi e delle infrastrutture informatiche e di comunicazione, gestione e assegnazione dei beni aziendali e delle risorse umane, delle apparecchiature per ufficio e di altri beni, pianificazione operativa e strategica, gestione dei progetti, continuità operativa, compilazione di audit trail e altri strumenti di rendicontazione, tenuta dei registri relativi alle attività aziendali, definizione del budget, gestione finanziaria e rendicontazione, comunicazioni, gestione di fusioni, acquisizioni, riorganizzazioni o cessioni, ecc.); e **(d) adempimento degli obblighi di legge applicabili e di altri requisiti** (ad es., obblighi in materia di protezione dei dati, imposte e previdenza sociale, prevenzione dei rischi e normativa sul lavoro, prevenzione delle frodi, segnalazione di illeciti, obblighi di conservazione dei documenti e di rendicontazione, esercizio di diritti e ricorso ai relativi mezzi di tutela, difesa in giudizio, garanzia del rispetto delle ispezioni governative e di altre richieste delle autorità governative o di altre autorità pubbliche, riscontro ad atti e procedimenti legali, quali mandati di comparizione, adempimento degli obblighi in materia di lavoro e previdenza sociale, svolgimento di audit e gestione di eventuali reclami o contestazioni interne, ecc.).

  Per quanto riguarda le **categorie particolari di dati personali** dei dipendenti **(compresi i dati personali relativi a condanne penali e reati, ove consentito)**, tali dati possono essere trattati dai Membri del Gruppo qualora ciò sia necessario per il corretto perseguimento delle relative finalità (ad

es., adempimento degli obblighi di legge, gestione delle risorse umane, gestione del canale di segnalazione degli illeciti, gestione delle paghe e dei benefit, gestione della mobilità interna, dei trasferimenti e dei distacchi, svolgimento in forma aggregata di segmentazioni, statistiche e analisi, ecc.) ed esclusivamente nella misura necessaria per assolvere gli obblighi ed esercitare i diritti specifici dei Membri del Gruppo o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (articolo 9, paragrafo 2, lettera b), del GDPR), nonché per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali (articolo 9, paragrafo 2, lettera h), del GDPR).

- I dati personali dei **familiari dei dipendenti** vengono trasferiti per finalità di gestione del trasferimento dei dipendenti all'estero, svolgimento in forma aggregata di segmentazioni, statistiche e analisi, nonché monitoraggio del rispetto del Codice di condotta sui mercati mobiliari o di politiche analoghe e dei relativi obblighi, tra cui l'approvazione e il monitoraggio delle operazioni su conti personali, e gestione dei benefit connessi ai diritti dei dipendenti (ad es., in ambito assicurativo).

- I dati personali dei **candidati attuali ed ex candidati** vengono trasferiti ai fini della gestione delle attività di selezione del personale a livello nazionale e internazionale (ad es., valutazione delle candidature e adozione delle decisioni di assunzione, comunicazioni con i candidati in merito al processo di selezione e/o alle relative candidature, ecc.).

- I dati personali dei **clienti potenziali e attuali** (compresi quelli dei loro dipendenti, rappresentanti e/o agenti, nonché utenti autorizzati e utenti del sito web) vengono trasferiti per le seguenti finalità: **(a) gestione del rapporto contrattuale con tali soggetti e fornitura dei nostri servizi** (ad es., emissione di carte di pagamento, anche a favore degli utenti autorizzati di carte aziendali, offerta e gestione dei nostri servizi di pagamento e di online banking, tenuta di registri per garantire la coerenza delle informazioni tra le diverse giurisdizioni, stipula di accordi e/o adozione di misure preliminari alla relativa conclusione, compresi i processi KYC, finalità aziendali e comunicazioni, trasferimenti di conto, instaurazione, rinnovo, mantenimento o cessazione dei rapporti commerciali, concessione dell'accesso alle attività basate su Internet e ai nostri locali, tenuta della documentazione aziendale, svolgimento di audit e analisi contabili, finanziarie ed economiche, esecuzione dei pagamenti e delle relative funzioni contabili, valutazione del rischio e del merito creditizio/della solvibilità, ecc.); **(b) gestione e garanzia della sicurezza** (ad es., protezione delle infrastrutture informatiche, delle apparecchiature per ufficio e di altri beni, ecc.); **(c) gestione delle attività operative aziendali** (ad es., tenuta dei registri dei dati relativi ai rappresentanti delle società o ad altri referenti, garanzia del coordinamento delle attività operative tra le diverse giurisdizioni, tenuta dei registri delle riunioni e degli altri rapporti commerciali, funzionamento e gestione dei sistemi informatici e di comunicazione, gestione dello sviluppo di prodotti e servizi, miglioramento dei prodotti e servizi, gestione dei beni aziendali, pianificazione strategica, gestione dei progetti, continuità operativa, compilazione di audit trail e di altri strumenti di rendicontazione, ecc.); **(d) rispetto della normativa applicabile** (ad es., obblighi in materia di protezione dei dati e fiscali, MiFID e valutazione dell'adeguatezza e dell'appropriatezza dei prodotti di investimento, prevenzione delle frodi, antiriciclaggio, obblighi di conservazione dei documenti e di rendicontazione, esercizio di diritti e ricorso ai relativi mezzi di tutela, difesa nell'ambito di controversie o procedimenti giudiziari, garanzia del rispetto delle ispezioni governative e di altre richieste delle autorità governative o di altre autorità pubbliche, riscontro ad atti e procedimenti legali, quali mandati di comparizione, ecc.); ed **(e) pianificazione e attuazione di strategie o campagne di marketing** (ad es., ricerche di mercato, pianificazione delle campagne e sviluppo di strategie di marketing, monitoraggio e rendicontazione dei risultati delle campagne, individuazione dei destinatari di prodotti/servizi, compresa la profilazione, previo consenso o nei casi consentiti dalla legge, ecc.).

Per quanto riguarda le **categorie particolari di dati personali** di clienti (compresi quelli dei rispettivi dipendenti, rappresentanti e/o agenti), **inclusi i dati personali relativi a condanne penali e reati, ove**

consentito, tali dati possono essere trattati dai Membri del Gruppo qualora ciò sia necessario per il corretto perseguimento delle relative finalità (ad es., adempimento degli obblighi di legge, individuazione di informazioni pubblicamente disponibili relative alle prassi adottate dai clienti nei rapporti con altre aziende che potrebbero incidere sul loro rapporto con la società, garanzia della coerenza delle informazioni tra le diverse giurisdizioni, rispetto delle ispezioni governative o giudiziarie e di altre richieste formulate da altre autorità pubbliche, ecc.) ed esclusivamente nella misura necessaria all'adempimento degli obblighi dei Membri del Gruppo o dell'interessato in materia di antiriciclaggio, prevenzione delle frodi, prevenzione dei reati e ambiti connessi, ove necessario e previsto o consentito dalla normativa applicabile.

- I dati personali dei **fornitori, venditori o prestatori di servizi attuali e potenziali** (compresi quelli dei loro dipendenti, rappresentanti e/o agenti) vengono trasferiti per le seguenti finalità: **(a) gestione del rapporto (pre)contrattuale con tali soggetti o con la loro società**, nel caso di persone giuridiche, **in generale** (ad es., svolgimento di verifiche dei livelli degli standard qualitativi, analisi del livello di rischio dei fornitori, analisi contabili, finanziarie ed economiche, adozione di misure preliminari alla conclusione degli accordi pertinenti, esecuzione degli accordi in essere, esecuzione dei pagamenti e delle relative funzioni contabili, finalità aziendali e comunicazioni, instaurazione, rinnovo, mantenimento o cessazione dei rapporti commerciali, tenuta della documentazione aziendale, ecc.); **(b) gestione e garanzia della sicurezza** (ad es., protezione delle infrastrutture informatiche, delle apparecchiature per ufficio e di altri beni, ecc.); **(c) gestione delle attività operative aziendali** (ad es., funzionamento e gestione dei sistemi informatici e di comunicazione, gestione dello sviluppo di prodotti e servizi, pianificazione strategica, gestione dei progetti, continuità operativa, compilazione di audit trail e di altri strumenti di rendicontazione, tenuta dei registri relativi alle attività aziendali, definizione del budget, gestione finanziaria e rendicontazione, comunicazioni, ecc.); e **(d) rispetto della normativa applicabile** (ad es., normativa commerciale e fiscale, prevenzione delle frodi, obblighi in materia di esternalizzazione applicabili agli enti finanziari, svolgimento di audit, rispetto delle ispezioni governative e di altre richieste delle autorità governative o di altre autorità pubbliche, esercizio di diritti e ricorso ai relativi mezzi di tutela, difesa in giudizio e gestione di eventuali reclami o contestazioni interne, ecc.).

- I dati personali degli **azionisti** vengono trasferiti per le seguenti finalità: **(a) gestione del rapporto con gli azionisti** (ad es., per finalità aziendali e comunicazioni, instaurazione, rinnovo, mantenimento o cessazione dei rapporti commerciali, gestione delle assemblee annuali e dei diritti degli azionisti, pagamento dei dividendi, tenuta della documentazione aziendale, concessione dell'accesso alle attività basate su Internet e ai locali, ecc.); e **(b) rispetto della normativa applicabile** (ad es., normativa commerciale e societaria, fiscale e in materia di valori mobiliari, svolgimento di audit, rispetto delle ispezioni governative e di altre richieste delle autorità governative o di altre autorità pubbliche, adempimento degli obblighi in materia di antiriciclaggio, certificazioni, esercizio di diritti e ricorso ai relativi mezzi di tutela, difesa in giudizio e gestione di eventuali reclami o contestazioni interne, ecc.).

- I dati personali degli **utenti web, utenti finali e utenti istituzionali (compresi quelli di piattaforme/siti web/app relativi al mondo universitario, al lavoro e all'imprenditorialità)** vengono trasferiti per le seguenti finalità: **(a) gestione della fornitura dei servizi in generale** (ad es., sviluppo e fornitura delle funzionalità e dei contenuti on-line, gestione dei siti web, gestione delle richieste di informazioni e di altro tipo, fornitura di assistenza, ecc.); **(b) gestione e garanzia della sicurezza** (ad es., protezione delle infrastrutture informatiche, garanzia della sicurezza e dell'integrità dei sistemi, dei server e dei siti web, ecc.); **(c) gestione delle attività operative aziendali** (ad es., garanzia del coordinamento delle attività operative tra le diverse giurisdizioni, tenuta dei registri delle riunioni e degli altri rapporti commerciali, miglioramento a livello globale dei processi relativi alle risorse umane e all'acquisizione di talenti, ecc.); **(d) pianificazione e attuazione di strategie o campagne di marketing** (ad es., ricerche di mercato, pianificazione delle campagne e sviluppo di strategie di marketing, monitoraggio e rendicontazione dei risultati delle campagne, individuazione dei

destinatari di prodotti/servizi, compresa la profilazione, previo consenso o nei casi consentiti dalla legge, ecc.); **(e) gestione delle attività di selezione del personale a livello nazionale e internazionale** (ad es., valutazione delle candidature e adozione delle decisioni di assunzione, comunicazioni con i candidati in merito al processo di selezione e/o alle relative candidature, ecc.); **(f) svolgimento in forma aggregata di segmentazioni, statistiche e analisi** (ad es., comprensione delle modalità di utilizzo dei servizi, miglioramento e sviluppo delle funzionalità dei siti web e dei servizi, miglioramento delle prestazioni e dell'assistenza disponibile, ecc.); e **(g) rispetto della normativa applicabile** (ad es., normativa commerciale, svolgimento di audit, rispetto delle ispezioni governative e di altre richieste delle autorità governative o di altre autorità pubbliche, riscontro ad atti e procedimenti legali, quali mandati di comparizione, esercizio di diritti e ricorso ai relativi mezzi di tutela, difesa in giudizio e gestione di eventuali reclami o contestazioni interne, ecc.).

I dati personali elencati nelle presenti Norme vengono inoltre trasferiti tra i Membri del Gruppo, nella misura necessaria alla **fornitura reciproca di un'ampia gamma di servizi interni** (ad es., tecnologie e sistemi informatici, servizi di back office, selezione e gestione delle risorse umane, audit interno e conformità normativa, gestione del canale di segnalazione degli illeciti, servizio centralizzato di posta per le candidature e i dipendenti, tecnologie di pagamento e servizi di elaborazione dei pagamenti, servizi di autorizzazione e acquisizione delle operazioni con carte di credito, servizi di fatturazione e determinazione dei prezzi, distruzione e trasporto di documenti, gestione dei rischi, approvvigionamento di prodotti e/o servizi, fatturazione elettronica, gestione del marketing e delle comunicazioni, nonché servizi di gestione e coordinamento in ambito legale in determinati settori, quali la protezione dei dati, ecc.).

ULTERIORI INFORMAZIONI

Il Gruppo Santander ha nominato dei responsabili della protezione dei dati (RPD o DPO) e/o referenti per la protezione dei dati (Champion) (come definiti di seguito), che coordinano i team locali, garantiscono la conformità normativa a livello locale nelle diverse società del Gruppo in tutto il mondo e fanno parte del Team Privacy del Gruppo Santander (anch'esso definito di seguito). Per qualsiasi domanda relativa alle disposizioni delle presenti Norme, ai diritti riconosciuti dalle stesse o a qualsiasi altra questione in materia di protezione dei dati, è possibile contattare l'RPD/il referente per la protezione dei dati all'indirizzo indicato di seguito. L'RPD/il referente per la protezione dei dati provvederà a gestire direttamente la questione, a trasmetterla alla persona o all'ufficio designato all'interno del Gruppo Santander oppure, ove opportuno, a sottoporla alla persona o all'organo competente.

Alla cortese attenzione del: Team Privacy

E-mail: l'elenco degli indirizzi e-mail pertinenti è disponibile qui.

In caso di dubbi sulle modalità con cui un Membro del Gruppo potrebbe aver trattato dei dati personali, è prevista una specifica procedura di gestione dei reclami, illustrata nella Parte III (cfr. **Appendice 2**).

PARTE II: OBBLIGHI DEI MEMBRI DEL GRUPPO

La Parte II delle presenti Norme è suddivisa in tre sezioni:

- La Sezione A tratta i principi fondamentali in materia di protezione dei dati, in linea con quelli previsti dalla normativa europea sulla protezione dei dati, che ciascun Membro del Gruppo è tenuto a rispettare.

- La Sezione B riguarda gli impegni concreti assunti dai Membri del Gruppo nei confronti delle autorità di controllo competenti in relazione alle presenti Norme.

- La Sezione C descrive i diritti dei terzi beneficiari riconosciuti dai Membri del Gruppo agli interessati ai sensi della Parte II delle presenti Norme.

SEZIONE A: PRINCIPI DI BASE

NORMA 1 – LICEITÀ E CORRETTEZZA

Norma 1A – I Membri del Gruppo rispetteranno le presenti Norme e qualsiasi normativa locale applicabile in materia di protezione dei dati in modo armonizzato.

In qualità di persone giuridiche, i Membri del Gruppo, fatto salvo quanto indicato di seguito, rispetteranno qualsiasi normativa applicabile in materia di dati personali (ad es., in Europa, la normativa europea sulla protezione dei dati) e garantiranno che il trattamento dei dati personali avvenga in conformità alle presenti Norme e alla normativa locale applicabile in materia di protezione dei dati.

Qualora trovino applicazione le presenti Norme e:

- non esista una normativa locale applicabile in materia di protezione dei dati oppure tale normativa non soddisfi gli standard stabiliti dalle disposizioni contenute nelle presenti Norme, i Membri del Gruppo tratteranno i dati personali in conformità alle presenti Norme, attenendosi alle disposizioni ivi stabilite;

- la normativa locale applicabile in materia di protezione dei dati richieda un livello di protezione superiore a quello previsto dalle presenti Norme, prevarrà il livello di protezione superiore, purché continuino a essere rispettati i diritti e gli obblighi previsti dalle presenti Norme; oppure

- la normativa locale applicabile in materia di protezione dei dati impedisca ai Membri del Gruppo di adempiere agli obblighi previsti dalle presenti Norme o incida in misura sostanziale sulla loro capacità di rispettarli, i Membri del Gruppo seguiranno la procedura descritta nella Norma 13.

Norma 1B – I Membri del Gruppo garantiranno che il trattamento dei dati personali sia lecito e corretto e che, ove richiesto, sussista una base giuridica per tale trattamento.

I Membri del Gruppo garantiranno che il trattamento dei dati personali sia corretto e lecito e che, ove richiesto, sussista una base giuridica per tale trattamento. In conformità alla normativa europea sulla protezione dei dati, i Membri del Gruppo tratteranno i dati personali esclusivamente qualora:

- l'interessato abbia prestato il proprio consenso al trattamento dei suoi dati personali e tale consenso soddisfi i requisiti previsti dalla normativa europea sulla protezione dei dati (ossia sia libero, specifico, informato e inequivocabile); oppure

- il trattamento sia necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; oppure

- il trattamento sia necessario per adempiere un obbligo legale al quale è soggetto il Membro del Gruppo (purché tale normativa soddisfi, ove applicabili, i requisiti previsti dalla Norma 13 di seguito); oppure

- il trattamento sia necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica; oppure

- il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui sia investito un Membro del Gruppo, purché tale compito sia previsto da una normativa che soddisfi, ove applicabili, i requisiti stabiliti dalla Norma 13 di seguito; oppure

- il trattamento sia necessario per il perseguimento del legittimo interesse di un Membro del Gruppo o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

Qualora il trattamento riguardi dati personali relativi a condanne penali e reati o a connesse misure di sicurezza, i Membri del Gruppo procederanno a tale trattamento esclusivamente sotto il controllo dell'autorità pubblica o quando esso sia autorizzato dalla legge, che preveda garanzie adeguate per i diritti e le libertà degli interessati, conformemente alle basi giuridiche sopra indicate.

Norma 1C – Fatto salvo quanto previsto dalla Norma 1B di cui sopra, è vietato trattare categorie particolari di dati personali, salvo che trovi applicazione una deroga, come quelle previste dalla normativa europea sulla protezione dei dati.

Il trattamento di categorie particolari di dati personali è consentito esclusivamente in presenza di determinati presupposti:

- il Membro del Gruppo abbia ottenuto il consenso esplicito dell'interessato al trattamento di categorie particolari di dati personali che lo riguardano per una o più finalità specifiche, salvo che una disposizione di legge stabilisca che il divieto di trattare tali dati non possa essere revocato dall'interessato; oppure

- il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del Membro del Gruppo o dell'interessato in materia di diritto del lavoro, della sicurezza sociale e della protezione sociale, nella misura in cui sia autorizzato dalla legge o da un contratto collettivo ai sensi della legge, che prevedano garanzie appropriate per i diritti fondamentali e gli interessi degli interessati; oppure

- il trattamento sia necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; oppure

- il trattamento sia effettuato, nell'ambito delle sue legittime attività e con garanzie adeguate, da una fondazione, un'associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che riguardi esclusivamente i membri o gli ex membri dell'organismo oppure persone che abbiano con esso contatti regolari in relazione alle sue finalità e che i dati personali non siano comunicati all'esterno dell'organismo senza il consenso degli interessati; oppure

- il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato; oppure

- il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria oppure ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; oppure

- il trattamento sia necessario per motivi di interesse pubblico rilevante sulla base di una disposizione di legge, purché sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; oppure

- il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro, per la valutazione della capacità lavorativa del dipendente, per la diagnosi, l'assistenza o la terapia sanitaria o sociale ovvero per la gestione dei sistemi e servizi sanitari o sociali, sulla base di una disposizione di legge, purché sia effettuato da o sotto la responsabilità di un professionista soggetto all'obbligo di segretezza previsto dalla legge o dalle norme stabilite dagli organismi nazionali competenti; oppure

- il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità pubblica, sulla base di una disposizione di legge che preveda misure appropriate e specifiche per tutelare i diritti e le libertà degli interessati, in particolare l'obbligo del segreto professionale; oppure

- il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sulla base di una disposizione di legge che sia proporzionata alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Norma 1D – I membri del Gruppo valuteranno l'impatto di qualsiasi trattamento di dati personali che comporti rischi elevati per i diritti e le libertà degli interessati.

Gli Esportatori, quando agiscono in qualità di titolari del trattamento, valuteranno la necessità e la proporzionalità di qualsiasi nuovo trattamento di dati personali e, qualora questo possa presentare un rischio elevato per i diritti e le libertà degli interessati, effettueranno una valutazione d'impatto sulla protezione dei dati conformemente alla normativa europea sulla protezione dei dati. Qualora dalla valutazione d'impatto sulla protezione dei dati emerga che il trattamento comporterebbe un rischio elevato per gli interessati, gli Esportatori saranno tenuti, in assenza di misure adottate per attenuare tale rischio, a consultare le autorità di controllo competenti prima di iniziare il trattamento.

NORMA 2 – GARANTIRE LA TRASPARENZA E TRATTARE I DATI PERSONALI ESCLUSIVAMENTE PER UNA FINALITÀ NOTA

Norma 2A – I Membri del Gruppo informeranno gli interessati in merito alle modalità di trattamento dei loro dati.

I Membri del Gruppo garantiranno che gli interessati siano sempre informati in modo chiaro ed esaustivo, generalmente mediante un'informativa sul trattamento dei dati personali, in merito alle modalità di trattamento dei loro dati personali. Il Membro del Gruppo competente fornirà le informazioni richieste dalla normativa europea sulla protezione dei dati, che comprenderanno almeno quanto segue:

- l'identità e i dati di contatto del titolare del trattamento, compresi, ove applicabile, i dati di contatto del responsabile della protezione dei dati e del rappresentante;

- le finalità e la base giuridica del trattamento, compresa una spiegazione di qualsiasi trattamento fondato sul legittimo interesse e di eventuali finalità nuove, diverse e compatibili;

- i destinatari o le categorie di destinatari dei dati personali;

- informazioni sulle garanzie predisposte per proteggere i dati personali in caso di trasferimento internazionale e sulle modalità per consultare od ottenere una copia di tali garanzie. In caso di trasferimenti di dati personali tra un Esportatore e un Importatore basati sulle presenti Norme, le informazioni fornite comprenderanno un riferimento alle presenti Norme e alle relative modalità di consultazione;

- il periodo di conservazione dei dati personali oppure i criteri utilizzati per determinarlo;

- informazioni dettagliate sui diritti degli interessati, compresi il diritto di accesso, di rettifica, alla cancellazione, alla limitazione del trattamento, di opposizione e alla portabilità dei dati, nonché il diritto di revocare il consenso, qualora il trattamento sia basato sul consenso, e il diritto di proporre reclamo a un'autorità di controllo;

- se il conferimento dei dati personali costituisca un obbligo legale o contrattuale e quali siano le conseguenze dell'eventuale mancato conferimento in tali circostanze; e

- informazioni sull'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno nei casi in cui tali decisioni producano effetti giuridici che riguardano l'interessato o incidano in modo analogo significativamente sulla sua persona, oppure siano basate su categorie particolari di dati personali, informazioni significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste di tale trattamento per l'interessato.

I requisiti della normativa locale applicabile in materia di protezione dei dati vigente nel luogo in cui i dati personali sono raccolti determineranno se sia necessario fornire ulteriori informazioni agli interessati.

Tali informazioni saranno fornite al momento in cui i Membri del Gruppo ottengono i dati personali dall'interessato oppure entro un diverso termine consentito dalla normativa europea sulla protezione dei dati.

Qualora i Membri del Gruppo ottengano i dati personali dell'interessato da una fonte diversa dall'interessato stesso, il Membro del Gruppo competente fornirà tali informazioni all'interessato, unitamente alle informazioni sulla fonte e sulle categorie di dati personali ricevuti da terzi, secondo le seguenti modalità:

- entro un termine ragionevole dall'ottenimento dei dati personali e comunque non oltre un (1) mese;

- qualora i dati personali siano destinati a essere trattati ai fini della comunicazione con l'interessato, al più tardi al momento della prima comunicazione con quest'ultimo; oppure

- qualora sia prevista la comunicazione dei dati personali a terzi, al più tardi al momento della prima comunicazione.

I Membri del Gruppo si atterranno alla presente Norma 2A, salvo che la mancata comunicazione delle informazioni sia espressamente consentita dalla normativa europea sulla protezione dei dati.

Norma 2B – I Membri del Gruppo otterranno e tratteranno i dati personali esclusivamente per le finalità note all'interessato o compatibili con le sue aspettative e pertinenti per i Membri del Gruppo.

La Norma 1A stabilisce che i Membri del Gruppo rispetteranno qualsiasi normativa applicabile relativa al trattamento dei dati personali, purché soddisfi, ove applicabili, i requisiti previsti dalla Norma 13, riportata di

seguito. Ciò significa che i Membri del Gruppo raccoglieranno dati personali per finalità specifiche, esplicite e legittime e non li tratteranno ulteriormente in modo incompatibile con tali finalità.

I Membri del Gruppo individueranno e renderanno note le finalità per le quali saranno trattati i dati personali, compresi gli utilizzi secondari e le comunicazioni dei dati, conformemente alla Norma 2A.

Norma 2C – I Membri del Gruppo potranno trattare i dati personali per una finalità diversa o nuova esclusivamente qualora sia compatibile con la finalità per la quale sono stati raccolti.

Qualora un Membro del Gruppo raccolga dati personali per una finalità specifica conformemente alla Norma 2A (come comunicato all'interessato mediante la relativa informativa sul trattamento dei dati personali) e secondo quanto descritto nella Norma 2B e intenda successivamente trattarli per una finalità diversa o nuova, non procederà a un ulteriore trattamento incompatibile con la finalità per la quale sono stati raccolti, salvo che tale ulteriore trattamento si basi sul consenso dell'interessato o sia richiesto dalla legge, purché tale legge soddisfi, ove applicabili, i requisiti previsti dalla Norma 13, riportata di seguito.

NORMA 3 – GARANTIRE LA QUALITÀ DEI DATI

Norma 3A – I Membri del Gruppo manterranno i dati personali esatti e aggiornati.

Al fine di garantire che i dati personali detenuti dai Membri del Gruppo siano esatti e aggiornati, i Membri del Gruppo invitano attivamente gli interessati a informarli di eventuali modifiche dei propri dati personali. I Membri del Gruppo adotteranno misure ragionevoli per garantire che i dati personali inesatti rispetto alle finalità per le quali sono trattati siano cancellati o rettificati senza indugio.

Norma 3B – I Membri del Gruppo conserveranno i dati personali solo per il tempo strettamente necessario al conseguimento delle finalità per le quali sono trattati.

I Membri del Gruppo rispetteranno la normativa applicabile a ciascuno di essi, nonché le politiche e le procedure del Gruppo Santander in materia di conservazione della documentazione, come di volta in volta rivista e aggiornata. Ciò significa, tra l'altro, che i Membri del Gruppo cancelleranno o bloccheranno, a seconda dei casi, i dati personali che non siano più necessari per le finalità per le quali sono stati raccolti e successivamente trattati.

Norma 3C – I Membri del Gruppo tratteranno esclusivamente dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

I Membri del Gruppo tratteranno esclusivamente i dati personali necessari per conseguire correttamente le finalità per le quali sono trattati.

NORMA 4 – ADOTTARE MISURE DI SICUREZZA ADEGUATE

Norma 4A – I membri del Gruppo rispetteranno le politiche di sicurezza informatica del Gruppo Santander.

I Membri del Gruppo adotteranno misure tecniche e organizzative adeguate per proteggere i dati personali dalla distruzione o dalla perdita accidentale o illecita, dall'alterazione, dalla comunicazione o dall'accesso non autorizzati, in particolare quando il trattamento comporta la trasmissione di dati personali attraverso una rete,

nonché da qualsiasi altra forma di trattamento illecito. A tal fine, i Membri del Gruppo rispetteranno i requisiti delle politiche di sicurezza vigenti all'interno del Gruppo Santander, come di volta in volta riviste e aggiornate, nonché qualsiasi altra procedura di sicurezza pertinente a un'area o funzione aziendale. Tenuto conto dello stato dell'arte e dei costi di attuazione, tali misure garantiranno un livello di sicurezza adeguato ai rischi connessi al trattamento e alla natura dei dati da proteggere.

Norma 4B – I Membri del Gruppo hanno adottato una politica di notifica delle violazioni dei dati.

I Membri del Gruppo hanno adottato procedure di risposta alle violazioni dei dati personali, come di volta in volta riviste e aggiornate, che definiscono il processo da seguire in caso di violazione della sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati ("**Violazione dei dati personali**").

In particolare, in caso di Violazione dei dati personali, la persona appartenente al Membro del Gruppo interessato che venga a conoscenza della violazione provvederà, senza ingiustificato ritardo, a notificarla:

- all'RPD o al referente per la protezione dei dati, tramite la funzione di controllo dei rischi operativi, ove applicabile;
- al Membro del Gruppo che agisce in qualità di titolare del trattamento, qualora il Membro del Gruppo interessato agisca in qualità di responsabile del trattamento; e
- al Membro responsabile per le violazioni.

L'RPD o il referente per la protezione dei dati valuterà, ove necessario con l'assistenza dell'Ufficio centrale per la protezione dei dati, se la Violazione dei dati personali debba essere notificata all'autorità di controllo competente. In tal caso, l'RPD o il referente per la protezione dei dati, a seconda dei casi, provvederà a notificare la Violazione dei dati personali all'autorità di controllo competente entro il termine previsto (conformemente alla normativa europea sulla protezione dei dati, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza).

Anche gli interessati saranno informati senza ingiustificato ritardo qualora la Violazione dei dati personali possa presentare un rischio elevato per i loro diritti e le loro libertà, salvo che tale comunicazione non sia richiesta ai sensi della normativa europea sulla protezione dei dati.

In linea con quanto precede, le Violazioni dei dati personali subite dai Membri del Gruppo, comprese le circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio, saranno inoltre registrate in Heracles, il registro degli incidenti di sicurezza del Gruppo Santander (comprese le Violazioni dei dati personali), che sarà messo a disposizione dell'autorità di controllo competente su richiesta.

Norma 4C – I Membri del Gruppo garantiranno che i fornitori di servizi e gli altri soggetti che trattano dati personali per loro conto adottino misure di sicurezza adeguate ed equivalenti.

I Membri del Gruppo che si avvalgono di un fornitore di servizi (che agisce in qualità di responsabile del trattamento) che abbia accesso ai dati personali degli interessati (ad es., un fornitore di servizi di elaborazione paghe), imporranno per iscritto al responsabile del trattamento obblighi contrattuali conformi ai requisiti della normativa europea sulla protezione dei dati, mediante un accordo vincolante sul trattamento dei dati. Tale accordo dovrà almeno prevedere quanto segue:

- l'oggetto e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati;

- gli obblighi e i diritti del titolare del trattamento;

- i seguenti obblighi a carico del soggetto che agisce in qualità di responsabile del trattamento:

    - trattare i dati personali esclusivamente sulla base di istruzioni documentate del titolare del trattamento, anche per quanto riguarda i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che ciò sia richiesto da una legge cui è soggetto il responsabile del trattamento, purché tale legge soddisfi, ove applicabili, i requisiti previsti dalla Norma 13, riportata di seguito. In tal caso, il responsabile del trattamento informerà il titolare del trattamento di tale obbligo giuridico prima di procedere al trattamento, salvo che la legge vieti tale informazione per rilevanti motivi di interesse pubblico;

    - garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o siano soggette a un adeguato obbligo legale di riservatezza;

    - adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio connesso al trattamento dei dati personali;

    - non ricorrere a un altro responsabile del trattamento in relazione ai dati personali senza la previa autorizzazione scritta, specifica o generale, del titolare del trattamento e stipulare, ove applicabile, un accordo scritto con l'ulteriore responsabile del trattamento, imponendogli gli stessi obblighi in materia di protezione dei dati previsti dal contratto o da altro atto giuridico tra il titolare e il responsabile del trattamento (in particolare, garanzie sufficienti circa l'adozione di misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti della normativa europea sulla protezione dei dati);

    - tenuto conto della natura del trattamento, assistere il titolare del trattamento mediante misure tecniche e organizzative adeguate, per quanto possibile, ai fini dell'adempimento dell'obbligo del titolare di dare seguito alle richieste di esercizio dei diritti degli interessati (ulteriormente descritti nella Norma 5, riportata di seguito);

    - assistere il titolare del trattamento nel garantire il rispetto degli obblighi relativi all'adozione di adeguate misure di sicurezza, alla realizzazione delle valutazioni d'impatto sulla protezione dei dati e delle relative consultazioni delle autorità di controllo competenti, nonché degli obblighi di notifica delle Violazioni dei dati personali alle autorità di controllo competenti e agli interessati, ove applicabile;

    - a scelta del titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali al termine della prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che la legge ne imponga la conservazione;

    - mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti per il responsabile del trattamento e consentire e contribuire alle attività di audit, comprese le ispezioni, svolte dal titolare del trattamento o da un altro revisore da questi incaricato; e

    - informare immediatamente il titolare del trattamento qualora ritenga che un'istruzione violi una disposizione di legge.

NORMA 5 – RISPETTARE I DIRITTI DEGLI INTERESSATI

Norma 5 – I Membri del Gruppo daranno seguito alle richieste degli interessati relative all'esercizio dei loro diritti in materia di protezione dei dati (compresi i diritti di accesso, rettifica, cancellazione, limitazione e portabilità dei dati personali, nonché il diritto di opposizione al trattamento dei dati personali e di revoca del consenso).

Su richiesta, gli interessati avranno il diritto di esercitare i seguenti diritti, secondo quanto previsto dalla normativa europea sulla protezione dei dati:

- diritto di accesso, che comporta la comunicazione di informazioni sui dati personali disponibili relativi all'interessato e la conferma che i suoi dati personali siano o meno oggetto di trattamento;

- diritto di rettifica, in virtù del quale l'interessato avrà il diritto di ottenere la rettifica dei dati personali inesatti o incompleti;

- diritto alla cancellazione o "diritto all'oblio", in virtù del quale l'interessato avrà il diritto di ottenere la cancellazione dei propri dati personali al ricorrere di determinate circostanze, quali quelle previste dall'articolo 17 del GDPR;

- diritto alla limitazione del trattamento, in virtù del quale l'interessato avrà il diritto di richiedere la limitazione del trattamento dei propri dati personali al ricorrere di determinate circostanze, quali quelle previste dall'articolo 18 del GDPR;

- diritto di ottenere che ciascun destinatario cui siano stati comunicati i dati personali sia informato di eventuali rettifiche o cancellazioni dei dati personali o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. L'interessato potrà inoltre chiedere di essere informato in merito a tali destinatari;

- diritto alla portabilità dei dati, in virtù del quale l'interessato avrà il diritto di ricevere in un formato strutturato i dati personali che lo riguardano e che ha fornito a un titolare del trattamento, nonché di trasmettere tali dati a un altro titolare del trattamento;

- diritto di opposizione, in virtù del quale l'interessato avrà il diritto di opporsi al trattamento dei propri dati personali per una finalità specifica, compreso il trattamento per finalità di marketing diretto e la profilazione nella misura in cui sia connessa a tale marketing;

- diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o incida in modo significativo sulla sua persona, ove applicabile; e

- diritto di revocare in qualsiasi momento il consenso prestato per uno specifico trattamento.

NORMA 6 – GARANTIRE UN'ADEGUATA PROTEZIONE DEI TRASFERIMENTI E DEI TRASFERIMENTI SUCCESSIVI

Norma 6 – I Membri del Gruppo non trasferiranno dati personali a terzi al di fuori dell'Europa senza garantire un'adeguata protezione degli stessi, conformemente agli standard stabiliti dalle presenti Norme e alla normativa europea sulla protezione dei dati.

I trasferimenti e i trasferimenti successivi di dati personali da parte di Membri del Gruppo soggetti alla normativa europea sulla protezione dei dati a terzi al di fuori dell'Europa non sono consentiti senza l'adozione delle misure appropriate previste da tale normativa europea.

Tali misure possono comprendere, tra l'altro:

- verificare che il terzo si trovi in un Paese per il quale la Commissione europea abbia riconosciuto un livello di protezione adeguato per i dati personali trasferiti; oppure

- sottoscrivere clausole contrattuali standard appropriate o ricorrere ad altri meccanismi previsti dalla normativa europea sulla protezione dei dati; oppure

- garantire che il trasferimento sia necessario per: (i) l'esecuzione di un contratto tra l'interessato e il Membro del Gruppo che effettua il trasferimento o l'esecuzione di misure precontrattuali adottate su richiesta dell'interessato; (ii) la conclusione o l'esecuzione di un contratto stipulato nell'interesse dell'interessato tra il Membro del Gruppo che effettua il trasferimento e un'altra parte; (iii) importanti motivi di interesse pubblico riconosciuti dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento; (iv) accertare, esercitare o difendere un diritto in sede giudiziaria; (v) tutelare gli interessi vitali dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità di prestare il proprio consenso; oppure (vi) ottenere il consenso esplicito degli interessati, dopo averli informati dei possibili rischi di tale trasferimento dovuti all'assenza di una decisione di adeguatezza e di garanzie adeguate.

SEZIONE B: IMPEGNI PRATICI

NORMA 7 – RISPETTO E RESPONSABILIZZAZIONE

Norma 7A – I Membri del Gruppo saranno responsabili del rispetto delle presenti Norme e saranno in grado di dimostrarlo; disporranno inoltre di personale e risorse adeguati per garantire e supervisionare il rispetto delle presenti Norme nell'ambito dell'intera attività aziendale.

Il Gruppo Santander dispone di una struttura organizzativa per la protezione dei dati incaricata di assumere decisioni, coordinare, attuare e supervisionare qualsiasi evento che possa verificarsi all'interno del Gruppo Santander in materia di protezione dei dati (il "**Privacy Team**"). La struttura per la protezione dei dati del Gruppo Santander è composta da:

- **Ufficio centrale per la protezione dei dati ("Ufficio DP centrale"):** organo aziendale responsabile della definizione dei criteri generali e della redazione delle politiche aziendali applicabili in materia di protezione dei dati. Insieme al team Rischi non finanziari, costituisce la seconda linea di difesa globale (2LoD), responsabile della supervisione della gestione delle attività connesse alla protezione dei dati svolte dalla prima linea di difesa (1LoD) e di garantire un'adeguata gestione dei rischi conformemente alla propensione al rischio del Gruppo Santander.

  In qualità di seconda linea di difesa globale, l'Ufficio DP centrale e il team Rischi non finanziari svolgono una serie di funzioni nei confronti di tutte le società del Gruppo Santander soggette alla normativa europea sulla protezione dei dati, tra cui principalmente:

  - Monitoraggio e controllo della conformità: (i) supervisione della conformità del Gruppo Santander in materia di protezione dei dati; (ii) rendicontazione consolidata all'alta dirigenza del Gruppo Santander; (iii) funzione di punto di contatto globale con le autorità di controllo

competenti, tramite i diversi RPD locali (o figure analoghe); (iv) analisi, insieme alle funzioni aziendali e di supporto competenti, dell'impatto degli incidenti di sicurezza a livello globale; (v) analisi e rendicontazione a livello globale dei rischi in materia di protezione dei dati; e (vi) definizione di criteri aziendali e funzione di punto di contatto all'interno del Gruppo per gli RPD/referenti per la protezione dei dati delle società del Gruppo (si veda di seguito).

- Funzione di supporto agli RPD e ai referenti per la protezione dei dati del Gruppo Santander (unità o soggetti centrali e soggetti locali). Principalmente, prestazione di consulenza specialistica in materia normativa e di supporto nello svolgimento delle funzioni di protezione dei dati a livello locale.

- **Struttura & governance**

  - **Banco Santander (Centrale)**: due figure principali forniscono supporto all'Ufficio DP centrale e riferiscono a quest'ultimo:

    - **RPD di Banco Santander** (formalmente designato dinanzi all'autorità di controllo spagnola): le sue funzioni all'interno della capogruppo, che l'RPD svolge in piena indipendenza, sono limitate a quelle descritte nel GDPR, che prevedono, tra l'altro, la sua partecipazione al dialogo con l'autorità di controllo spagnola. Fermi restando gli obblighi di rendicontazione e supporto dell'RPD nei confronti dell'Ufficio DP centrale, l'RPD riferisce direttamente al più alto livello dirigenziale di Banco Santander.

    - **Unità centrali**: unità designate nell'ambito dell'intera organizzazione. I loro principali ruoli e responsabilità consistono nel: (a) gestire e risolvere in prima istanza le questioni relative ai dati personali; (b) informare e fornire consulenza ai titolari del trattamento, ai responsabili del trattamento e ai dipendenti in merito alle modalità di rispetto della normativa applicabile in materia di protezione dei dati; (c) monitorare il rispetto della normativa in materia di protezione dei dati; (d) fungere da punto di contatto interno con funzione di supporto di primo livello; (e) trasmettere all'Ufficio DP centrale le richieste di informazioni e di supporto e comunicare gli indicatori di gestione.

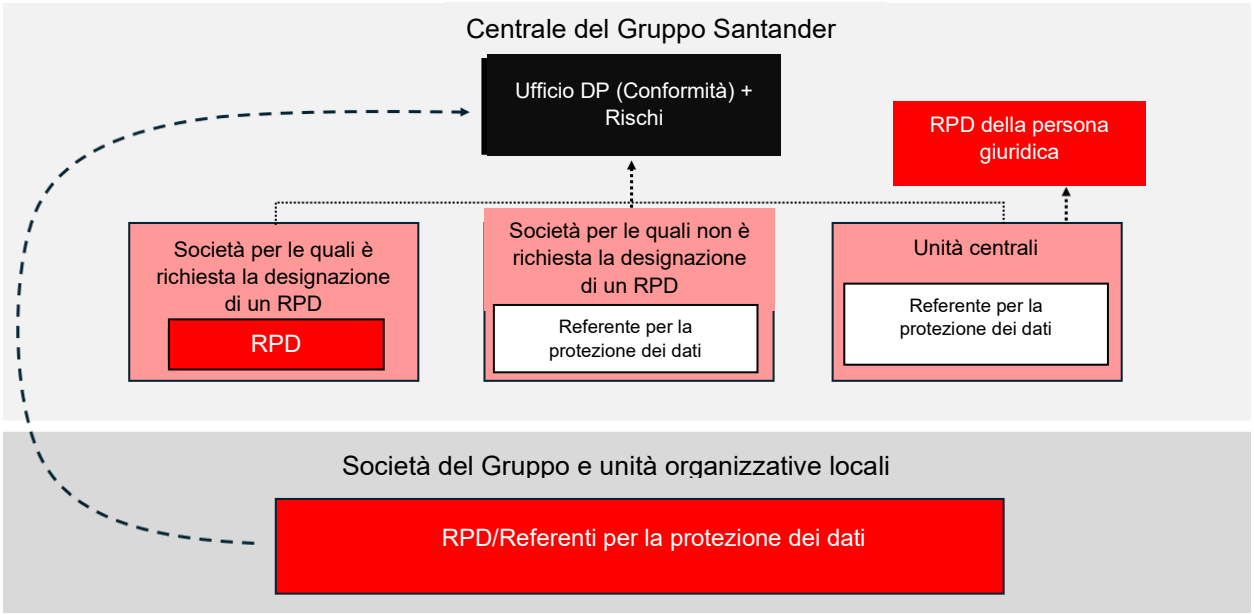
  - **Unità locali**: sono inoltre previste due figure che riferiscono all'Ufficio DP centrale:

    - **RPD (o figura locale analoga)**: ove richiesto dalla normativa locale applicabile in materia di protezione dei dati, viene designato un RPD (o una figura locale analoga). I suoi principali ruoli e responsabilità possono comprendere: (a) fungere da punto di contatto con l'autorità di controllo competente e con le parti interessate; (b) cooperare con l'autorità di controllo competente; (c) fornire consulenza in materia di protezione dei dati; (d) svolgere attività di monitoraggio e supervisione; (e) provvedere alla formazione; (f) fornire consulenza sulle valutazioni d'impatto sulla protezione dei dati; (g) effettuare le consultazioni preventive con l'autorità di controllo competente; (h) supervisionare i registri delle attività di trattamento; (i) fornire consulenza in merito alla notifica delle Violazioni dei dati personali; (j) fornire consulenza sulla gestione dei terzi; e (k) supervisionare l'esercizio dei diritti degli interessati.

    - **Referenti per la protezione dei dati o figure locali analoghe (es. privacy officer)**: qualora la normativa locale applicabile in materia di protezione dei dati non richieda la designazione di un RPD oppure, per le dimensioni e/o la complessità di una società del

Gruppo, sia necessario un numero elevato di RPD o di figure locali analoghe, l'Ufficio DP centrale può avvalersi del supporto di referenti locali per la protezione dei dati o figure analoghe (ad es., privacy officer), che riferiscono allo stesso. I loro ruoli e responsabilità sono molto simili a quelli degli RPD o delle figure analoghe, fatta eccezione per le comunicazioni con le autorità di controllo, alle quali non partecipano.

Lo schema sottostante illustra la struttura organizzativa e i rapporti tra le succitate figure responsabili della protezione dei dati nel Gruppo Santander:



Norma 7B – I Membri del Gruppo adotteranno misure tecniche e organizzative adeguate, fin dalla progettazione e di default, al fine di consentire e agevolare nella pratica il rispetto delle presenti Norme.

Tenuto conto dello stato dell'arte, dei costi di attuazione nonché dell'ambito di applicazione, della natura, del contesto e delle finalità del trattamento, i Membri del Gruppo adotteranno misure tecniche e organizzative adeguate che soddisfino i principi della protezione dei dati fin dalla progettazione e di default, come previsto dalla normativa europea sulla protezione dei dati. I Membri del Gruppo integreranno tali misure nel trattamento sia al momento di determinarne i mezzi sia durante il trattamento stesso, al fine di agevolare la protezione dei dati personali trattati e garantire che, di default, siano trattati esclusivamente i dati personali necessari per ciascuna specifica finalità del trattamento.

Norma 7C – I Membri del Gruppo che trattano dati personali terranno un registro scritto, anche in formato elettronico, delle proprie attività di trattamento e lo metteranno a disposizione delle autorità di controllo competenti su richiesta.

I registri delle attività di trattamento tenuti dai Membri del Gruppo che agiscono in qualità di titolari del trattamento conterranno:

- il nome e i dati di contatto del Membro del Gruppo e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

- le finalità del trattamento dei dati personali;
- una descrizione delle categorie di interessati i cui dati personali sono oggetto di trattamento e dei dati personali trattati;
- le categorie di destinatari ai quali i dati personali sono stati o saranno comunicati, compresi i destinatari in Paesi terzi od organizzazioni internazionali;
- informazioni dettagliate sul Paese terzo o sui Paesi terzi verso i quali sono trasferiti i dati personali, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate adottate per legittimare tali trasferimenti, salvo che il Paese sia stato dichiarato adeguato ai sensi della normativa europea sulla protezione dei dati;
- ove possibile, il periodo di conservazione dei dati personali; e
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate per proteggere i dati personali.

I registri delle attività di trattamento tenuti dai Membri del Gruppo che agiscono in qualità di responsabili del trattamento per conto di un Membro del Gruppo titolare del trattamento conterranno:

- i nomi e i dati di contatto del Membro del Gruppo e di ciascun titolare del trattamento per conto del quale agisce il responsabile del trattamento nonché, ove applicabile, del rappresentante del titolare o del responsabile del trattamento e del responsabile della protezione dei dati;
- le categorie di trattamenti effettuati per conto di ciascun titolare del trattamento;
- informazioni dettagliate sul Paese terzo o sui Paesi terzi verso i quali sono trasferiti i dati personali, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate adottate per legittimare tali trasferimenti, salvo che il Paese sia stato dichiarato adeguato ai sensi della normativa europea sulla protezione dei dati; e
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate per proteggere i dati personali.

I registri delle attività di trattamento tenuti dai Membri del Gruppo saranno redatti per iscritto, anche in formato elettronico, e messi a disposizione delle autorità di controllo competenti su richiesta.

NORMA 8 – FORMAZIONE

Norma 8 – I Membri del Gruppo forniranno una formazione adeguata ai dipendenti che hanno accesso permanente o regolare ai dati personali e/o che partecipano al trattamento dei dati personali o allo sviluppo di strumenti utilizzati per il trattamento di tali dati.

I Membri del Gruppo forniranno una formazione adeguata e aggiornata ai dipendenti che hanno accesso permanente o regolare ai dati personali e/o che partecipano al trattamento di tali dati o allo sviluppo di strumenti utilizzati per il loro trattamento. Tale formazione sarà erogata almeno una volta ogni due anni e riguarderà, tra l'altro, le procedure per la gestione delle richieste di accesso ai dati personali da parte delle autorità pubbliche.

NORMA 9 – AUDIT

Norma 9 – I Membri del Gruppo attueranno il Programma di audit riportato nell'Appendice 1.

I Membri del Gruppo attueranno il Programma di audit effettuando regolarmente audit interni e consentendo lo svolgimento di audit esterni, ove necessario, conformemente al processo formale di valutazione previsto dal Programma di audit. Gli esiti di tali audit saranno comunicati conformemente all'Appendice 1.

NORMA 10 – GESTIONE DEI RECLAMI

Norma 10 – I Membri del Gruppo attueranno la Procedura di gestione dei reclami riportata nell'Appendice 2.

I Membri del Gruppo attueranno la Procedura di gestione dei reclami prevista dall'Appendice 2, al fine di gestire adeguatamente i reclami degli interessati e garantire la tutela dei dati personali trattati dai Membri del Gruppo. I Membri del Gruppo consentiranno inoltre l'esercizio dei diritti dei terzi beneficiari previsti dalla Sezione C delle presenti Norme.

NORMA 11 – COOPERAZIONE CON LE AUTORITÀ DI CONTROLLO COMPETENTI

Norma 11 – I Membri del Gruppo attueranno la Procedura di cooperazione riportata nell'Appendice 3.

I Membri del Gruppo attueranno la Procedura di cooperazione riportata nell'Appendice 3 e coopereranno con le autorità di controllo competenti in relazione alle presenti Norme, accettando di essere sottoposti ad audit e ispezioni da parte delle stesse, anche in loco ove necessario; terranno inoltre conto delle loro indicazioni e si atterranno alle loro decisioni in merito a qualsiasi questione relativa alle presenti Norme.

NORMA 12 – AGGIORNAMENTO DELLE NORME

Norma 12 – I Membri del Gruppo attueranno la Procedura di aggiornamento riportata nell'Appendice 4.

I Membri del Gruppo attueranno la Procedura di aggiornamento riportata nell'Appendice 4 e comunicheranno senza ingiustificato ritardo, ove necessario, qualsiasi aggiornamento delle presenti Norme e dell'elenco dei Membri del Gruppo alle autorità di controllo competenti, agli interessati coinvolti e ai Membri del Gruppo.

NORMA 13 – MISURE DA ADOTTARE QUALORA LA LEGISLAZIONE NAZIONALE INCIDA SULLA CONFORMITÀ ALLE PRESENTI NORME

Norma 13A – I Membri del Gruppo si impegnano a utilizzare le presenti Norme come strumento per i trasferimenti verso gli Importatori soltanto qualora abbiano debitamente valutato che la legislazione e le prassi del Paese degli Importatori, compresi eventuali obblighi di comunicazione dei dati personali o misure che autorizzino l'accesso da parte delle autorità pubbliche, non impediscano loro di adempiere agli obblighi previsti dalle presenti Norme.

I Membri del Gruppo utilizzeranno le presenti Norme come strumento di tutela dei trasferimenti internazionali soltanto qualora abbiano valutato che la legislazione e le prassi dei Paesi terzi di destinazione interessati, compresi eventuali obblighi di comunicazione dei dati personali o misure che autorizzino l'accesso da parte delle autorità pubbliche, non impediscano loro di adempiere agli obblighi previsti dalle presenti Norme. Ciò si basa sul presupposto che le disposizioni legislative e le prassi che rispettano l'essenza dei diritti e delle libertà

fondamentali e non eccedono quanto necessario e proporzionato in una società democratica non siano in contrasto con le presenti Norme.

Nel valutare la legislazione e le prassi dei Paesi terzi che potrebbero incidere sul rispetto degli impegni contenuti nelle presenti Norme, i Membri del Gruppo terranno debitamente conto, in particolare, dei seguenti fattori:

(i) le circostanze specifiche del trasferimento o del complesso di trasferimenti e di eventuali trasferimenti successivi previsti all'interno dello stesso Paese terzo o verso un altro Paese terzo, tra cui:

- le finalità per le quali i dati sono trasferiti e trattati (ad es., marketing, risorse umane, conservazione, assistenza informatica, ecc.);
- le tipologie di soggetti coinvolti nel trattamento (l'Importatore ed eventuali ulteriori destinatari di trasferimenti successivi);
- il settore economico nel quale avviene il trasferimento o il complesso di trasferimenti;
- le categorie e il formato dei dati personali trasferiti;
- il luogo del trattamento, compresa la conservazione; e
- i canali di trasmissione utilizzati.

(ii) la legislazione e le prassi dei Paesi terzi di destinazione pertinenti alla luce delle circostanze del trasferimento. Queste possono comprendere: (a) quelle che impongono la comunicazione dei dati alle autorità pubbliche o autorizzano l'accesso da parte di tali autorità; (b) quelle che prevedono l'accesso a tali dati durante il transito tra i Paesi degli Esportatori e quelli degli Importatori; e (c) le limitazioni e le garanzie applicabili;

(iii) eventuali garanzie contrattuali, tecniche od organizzative pertinenti adottate a integrazione delle garanzie previste dalle presenti Norme. Ciò comprende le misure applicate durante la trasmissione e il trattamento dei dati personali nei Paesi di destinazione.

Qualora debbano essere adottate garanzie ulteriori rispetto a quelle previste dalle presenti Norme, il Membro responsabile per le violazioni e l'RPD o il referente per la protezione dei dati, a seconda dei casi, saranno informati e coinvolti nella valutazione. I Membri del Gruppo documenteranno adeguatamente tale valutazione, nonché le misure supplementari selezionate e attuate. Su richiesta, metteranno tale documentazione a disposizione dell'autorità di controllo competente.

Qualora le presenti Norme siano utilizzate come strumento per i trasferimenti, gli Importatori informeranno tempestivamente gli Esportatori se, per tutta la durata della loro adesione, abbiano motivo di ritenere di essere soggette o di essere divenute soggette a disposizioni legislative o prassi che impedirebbero loro di adempiere agli obblighi previsti dalle presenti Norme. Ciò comprende l'impossibilità di adempiere ai propri obblighi a seguito di una modifica della legislazione del Paese terzo interessato o di una misura, quale una richiesta di comunicazione dei dati. Tali informazioni dovranno essere fornite anche al Membro responsabile per le violazioni.

Una volta verificata tale notifica, l'Esportatore interessato, unitamente al Membro responsabile per le violazioni e all'RPD o al referente per la protezione dei dati, a seconda dei casi, si impegna a individuare tempestivamente le misure supplementari (ad es., misure tecniche od organizzative volte a garantire la sicurezza e la riservatezza) che l'Esportatore e/o l'Importatore dovranno adottare per poter adempiere agli obblighi previsti

dalle presenti Norme. Lo stesso vale qualora un Esportatore abbia motivo di ritenere che un Importatore non sia più in grado di adempiere ai propri obblighi previsti dalle presenti Norme.

Qualora l'Esportatore interessato, insieme al Membro responsabile per le violazioni e all'RPD o al referente per la protezione dei dati, a seconda dei casi, ritenga che le presenti Norme, anche se accompagnate da misure supplementari, non possano essere rispettate per un trasferimento o un complesso di trasferimenti, oppure qualora riceva istruzioni in tal senso dall'autorità di controllo competente, si impegna a sospendere il trasferimento o il complesso di trasferimenti in questione, nonché tutti i trasferimenti per i quali la medesima valutazione e le medesime motivazioni condurrebbero a un risultato analogo, fino a quando non sia nuovamente garantita la conformità o il trasferimento non venga interrotto.

A seguito di tale sospensione, l'Esportatore dovrà interrompere il trasferimento o il complesso di trasferimenti qualora non sia possibile rispettare le presenti Norme e la conformità non venga ripristinata entro un mese dalla sospensione. In tal caso, i dati personali trasferiti prima della sospensione e le relative copie dovranno, a scelta dell'Esportatore, essere restituiti o distrutti integralmente.

Il Membro responsabile per le violazioni e l'RPD o il referente per la protezione dei dati, a seconda dei casi, informeranno tutti gli altri Membri del Gruppo della valutazione effettuata e dei relativi risultati, affinché le misure supplementari individuate siano applicate qualora lo stesso tipo di trasferimenti venga effettuato da un altro Membro del Gruppo oppure, qualora non sia stato possibile adottare misure supplementari efficaci, i trasferimenti in questione siano sospesi o interrotti.

Gli Esportatori monitoreranno inoltre costantemente, ove opportuno in collaborazione con gli Importatori, gli sviluppi nei Paesi terzi verso i quali hanno trasferito dati personali che potrebbero incidere sulla valutazione iniziale del livello di protezione e sulle conseguenti decisioni relative a tali trasferimenti.

Norma 13B – Gli Importatori garantiranno che, qualora ricevano da un'autorità pubblica, ai sensi della legislazione del Paese di destinazione, una richiesta giuridicamente vincolante di comunicazione di dati personali trasferiti in conformità alle presenti Norme oppure vengano a conoscenza di un accesso diretto, da parte delle autorità pubbliche, ai dati personali trasferiti in conformità alle presenti Norme e ai sensi della legislazione del Paese di destinazione, ne informino tempestivamente l'Esportatore e, ove possibile, l'interessato, se necessario con l'assistenza dell'Esportatore.

Gli Importatori informeranno tempestivamente l'Esportatore interessato e, ove possibile, l'interessato, se necessario con l'assistenza dell'Esportatore, qualora:

- ricevano da un'autorità pubblica, ai sensi della legislazione del Paese di destinazione o di un altro Paese terzo, una richiesta giuridicamente vincolante di comunicazione di dati personali trasferiti in conformità alle presenti Norme (tale notifica dovrà comprendere informazioni sui dati personali richiesti, sull'autorità richiedente, sulla base giuridica della richiesta e sulla risposta fornita); oppure

- vengano a conoscenza di un accesso diretto, da parte delle autorità pubbliche, ai dati personali trasferiti in conformità alle presenti Norme e ai sensi della legislazione del Paese di destinazione (tale notifica dovrà comprendere tutte le informazioni a disposizione dell'Importatore).

Qualora gli sia vietato informare l'Esportatore e/o l'interessato in merito all'accesso, l'Importatore si adopererà al meglio per ottenere la revoca del divieto, al fine di comunicare all'Esportatore il maggior numero di

informazioni nel più breve tempo possibile, e documenterà gli sforzi compiuti per poterli dimostrare su richiesta dell'Esportatore.

L'Importatore fornirà periodicamente all'Esportatore quante più informazioni pertinenti possibile in merito alle richieste ricevute, in particolare il numero di richieste, il tipo di dati richiesti, l'autorità o le autorità richiedenti, l'eventuale contestazione delle richieste e l'esito di tali contestazioni, ecc. Qualora all'Importatore sia o divenga parzialmente o totalmente vietato fornire all'Esportatore le informazioni sopra indicate, ne informerà quest'ultimo senza ingiustificato ritardo.

L'Importatore conserverà le informazioni sopra indicate per tutto il periodo in cui i dati sono soggetti alle garanzie previste dalle presenti Norme e le metterà a disposizione dell'autorità di controllo competente su richiesta.

L'Importatore valuterà la legittimità della richiesta di comunicazione, verificando in particolare se rientri nei poteri conferiti all'autorità pubblica richiedente, e la contesterà qualora, a seguito di un'attenta valutazione, concluda che sussistono ragionevoli motivi per ritenere che sia illegittima ai sensi della legislazione del Paese di destinazione, degli obblighi applicabili previsti dal diritto internazionale e dei principi di cortesia internazionale. Alle medesime condizioni, l'Importatore esperirà le possibilità di ricorso disponibili. Nel contestare una richiesta, l'Importatore chiederà l'adozione di misure cautelari volte a sospenderne gli effetti fino a quando l'autorità giudiziaria competente non si sia pronunciata nel merito. L'Importatore non comunicherà i dati personali richiesti fino a quando non sia tenuto a farlo ai sensi delle norme procedurali applicabili.

L'Importatore documenterà la propria valutazione giuridica e l'eventuale contestazione della richiesta di comunicazione e, nella misura consentita dalla legislazione del Paese di destinazione, metterà tale documentazione a disposizione dell'Esportatore. La metterà inoltre a disposizione dell'autorità di controllo competente su richiesta.

Nel rispondere a una richiesta di comunicazione, l'Importatore fornirà la quantità minima di informazioni consentita, sulla base di un'interpretazione ragionevole della richiesta.

In ogni caso, i Membri del Gruppo garantiranno che gli eventuali trasferimenti di dati personali a un'autorità pubblica effettuati ai sensi delle presenti Norme non avvengano su vasta scala e non siano sproporzionati o indiscriminati, in misura eccedente quanto necessario in una società democratica.

NORMA 14 – INOSSERVANZA DELLE NORME E CESSAZIONE DEI TRASFERIMENTI

Norma 14A – Gli Esportatori trasferiranno dati personali esclusivamente agli Importatori che siano effettivamente vincolati dalle presenti Norme e siano in grado di garantirne la conformità.

Nessun trasferimento ai sensi delle presenti Norme sarà effettuato a favore di un Membro del Gruppo, a meno che tale Membro sia effettivamente vincolato dalle presenti Norme e sia in grado di garantirne la conformità. Qualora, per qualsiasi motivo, un Importatore non sia in grado di rispettare le presenti Norme, ne informerà tempestivamente l'Esportatore. Qualora l'Importatore violi le presenti Norme o non sia in grado di rispettarle, l'Esportatore sospenderà o non effettuerà il trasferimento.

L'Importatore, a scelta dell'Esportatore, restituirà o cancellerà immediatamente e integralmente i dati personali trasferiti ai sensi delle presenti Norme qualora:

- l'Esportatore abbia sospeso il trasferimento e la conformità alle presenti Norme non sia ripristinata entro un termine ragionevole e, in ogni caso, entro un mese dalla sospensione; oppure

- l'Importatore violi in modo sostanziale o persistente le presenti Norme; oppure
- l'Importatore non rispetti una decisione vincolante di un'autorità giudiziaria o di un'autorità di controllo competente in merito agli obblighi ad esso incombenti ai sensi delle presenti Norme.

Lo stesso si applicherà a eventuali copie dei dati. L'Importatore certificherà all'Esportatore l'avvenuta cancellazione dei dati. Fino alla cancellazione o alla restituzione dei dati, l'Importatore continuerà a garantire la conformità alle presenti Norme. Qualora sussista un divieto di legge che impedisca all'Importatore di restituire o cancellare i dati personali trasferiti, l'Importatore garantisce che continuerà ad assicurare la conformità alle presenti Norme e tratterà i dati esclusivamente nella misura e per il tempo previsti dalla legge.

Norma 14B – L'Importatore che cessi di essere vincolato dalle presenti Norme garantirà che i dati personali siano adeguatamente conservati, restituiti o cancellati, a seconda dei casi.

L'Importatore che cessi di essere vincolato dalle presenti Norme potrà conservare, restituire o cancellare, a seconda dei casi, i dati personali ricevuti ai sensi delle presenti Norme. Qualora l'Esportatore e l'Importatore concordino che i dati possano essere conservati dall'Importatore, dovrà essere mantenuta la protezione prevista dalle presenti Norme.

SEZIONE C: DIRITTI DEI TERZI BENEFICIARI

C.1 Gli interessati i cui dati personali sono trasferiti a un Importatore devono poter beneficiare di determinati diritti in qualità di terzi beneficiari. A tal fine, gli interessati possono far valere il rispetto delle seguenti disposizioni:

- Norme 1B e 1C (in materia di correttezza e liceità e di trattamento di categorie particolari di dati personali);
- Norma 2 (in materia di trasparenza e di trattamento dei dati personali esclusivamente per una finalità nota);
- Norma 3 (in materia di minimizzazione ed esattezza dei dati e di limitazione dei periodi di conservazione);
- Norma 4 (in materia di misure di sicurezza adeguate e di obblighi di notifica delle violazioni dei dati personali);
- Norma 5 (in materia di rispetto dei diritti degli interessati);
- Norma 6 (in materia di protezione adeguata in caso di trasferimenti e trasferimenti successivi);
- Norma 10 (in materia di gestione dei reclami);
- Norma 11 (in materia di cooperazione con le autorità di controllo competenti);
- Norma 12 (in materia di aggiornamento delle Norme);
- Norma 13 (in materia di misure da adottare qualora la legislazione nazionale impedisca la conformità alle presenti Norme);

- le disposizioni di cui ai punti da C1 a C3, che conferiscono diritti ai terzi beneficiari e stabiliscono le norme in materia di responsabilità e giurisdizione ai sensi delle presenti Norme; e

- il diritto di accedere alle presenti Norme, disponibili sulla pagina web, nella rete interna della società (accessibile ai dipendenti), o di ottenerne una copia cartacea, nonché di ottenere un elenco dei Membri del Gruppo vincolati dalle presenti Norme.

mediante:

- *la presentazione di un reclamo*: gli interessati possono presentare reclamo a un Membro del Gruppo (conformemente alla Procedura di gestione dei reclami riportata nell'Appendice 2) e all'autorità di controllo dello Stato membro nel quale si è verificata la presunta violazione o nel quale l'interessato lavora o risiede abitualmente; e/o

- *l'avvio di un procedimento giudiziario*: gli interessati possono agire in giudizio contro i Membri del Gruppo dinanzi agli organi giurisdizionali dello Stato membro nel quale il Membro del Gruppo ha uno stabilimento o dello Stato membro nel quale l'interessato ha la propria residenza abituale.

Come ulteriormente precisato ai punti da C.2 a C.4, qualora una violazione sia commessa da un Membro del Gruppo situato al di fuori del SEE, gli interessati conserveranno il diritto di presentare reclamo e agire in giudizio nei confronti del Membro responsabile per le violazioni designato, come se la violazione fosse stata commessa da tale soggetto nello Stato membro in cui è stabilito.

Tali diritti non si estendono ai punti delle presenti Norme relativi ai meccanismi interni attuati presso i Membri del Gruppo, quali le informazioni dettagliate sulla formazione, sul Programma di audit, sulla rete per la conformità e sul meccanismo per il loro aggiornamento.

Inoltre, i Membri del Gruppo accettano che gli interessati possano essere rappresentati da un organismo, un'organizzazione o un'associazione senza scopo di lucro alle condizioni stabilite dall'articolo 80, paragrafo 1, del GDPR.

C.2 Gli interessati possono inoltre chiedere un adeguato risarcimento al Membro responsabile per le violazioni, il quale si impegna ad adottare le misure necessarie per porre rimedio a qualsiasi violazione, da parte di un Importatore, delle disposizioni elencate al punto C.1 e, ove opportuno, a risarcire gli interessati per qualsiasi danno, materiale o immateriale, subito a seguito della violazione, da parte di un Importatore, di una o più delle disposizioni elencate al punto C.1, conformemente a quanto stabilito da un'autorità giudiziaria o da un'altra autorità competente.

C.3 A scanso di equivoci, gli interessati beneficeranno dei diritti dei terzi beneficiari descritti nella presente Sezione C e gli organi giurisdizionali europei o le autorità di controllo competenti avranno giurisdizione come se la violazione di una o più delle disposizioni descritte nella presente Sezione C fosse stata commessa dal Membro responsabile per le violazioni.

C.4 Qualora sia presentato un reclamo nel quale un interessato sostenga di aver subito un danno a seguito di una violazione delle presenti Norme, i Membri del Gruppo convengono che spetterà al Membro responsabile per le violazioni dimostrare che l'Importatore non è responsabile della violazione o che tale violazione non si è verificata.

PARTE III: APPENDICI

APPENDICE 1

PROGRAMMA DI AUDIT

1. INTRODUZIONE

1.1 I Membri del Gruppo sono tenuti a verificare mediante audit la propria conformità alle presenti Norme e, nello svolgimento di tali audit, devono soddisfare determinate condizioni. Il presente documento descrive le modalità con cui i Membri del Gruppo adempiono a tali requisiti.

1.2 Le *attività ordinarie* (BAU) degli RPD e dei referenti per la protezione dei dati comprendono la fornitura di indicazioni sul trattamento dei dati personali soggetto alle presenti Norme e la valutazione dei trattamenti di dati personali effettuati dai Membri del Gruppo, al fine di individuare potenziali rischi per la privacy nell'attività quotidiana. Il trattamento dei dati personali è pertanto oggetto di un esame e di una valutazione dettagliati e continuativi.

1.3 In qualità di seconda linea di difesa (2LoD) a livello globale, l'Ufficio DP centrale svolge le attività di monitoraggio e controllo, compresa la supervisione della conformità del Gruppo Santander in materia di protezione dei dati.

1.4 Il Programma di audit consiste invece nella valutazione formale e indipendente effettuata dalla terza linea di difesa (3LoD) per garantire la conformità alle presenti Norme, come richiesto dalle autorità di controllo competenti. Il parere espresso dalla funzione di audit (3LoD) è indipendente e non sostituisce le responsabilità di controllo e supervisione della prima e della seconda linea di difesa (1LoD e 2LoD), che rientreranno anch'esse nell'ambito dell'audit in sede di verifica dell'integrazione e dell'attuazione delle presenti Norme.

2. APPROCCIO

2.1 Panoramica dell'audit

Il soggetto responsabile dell'esecuzione degli audit sulla conformità alle presenti Norme e di garantire che tali audit ne esaminino tutti gli aspetti può variare in funzione delle circostanze specifiche di ciascun Membro del Gruppo. Di norma, gli audit sono supervisionati, a seconda dei casi, da auditor interni o esterni accreditati, la cui indipendenza nello svolgimento delle relative funzioni è garantita. L'auditor competente avrà la responsabilità di garantire che eventuali criticità o casi di non conformità siano portati all'attenzione dell'alta dirigenza e che le azioni correttive necessarie per garantire la conformità siano attuate entro un termine ragionevole.

2.2 Tempistica e ambito dell'audit

2.2.1 La funzione di Audit interno, conformemente alla propria metodologia di valutazione dei rischi, stabilirà la tempistica degli audit nell'ambito di un ciclo massimo di quattro anni.

I primi audit saranno tuttavia effettuati entro i primi 24 mesi dall'approvazione formale delle presenti Norme e dalla conseguente entrata in vigore delle stesse. Successivamente, l'audit sarà effettuato secondo la metodologia di audit basata sul rischio applicabile, come indicato nel primo paragrafo del presente punto 2.2.

In ogni caso, i Membri del Gruppo saranno tenuti a effettuare un audit qualora (i) vi siano indizi di non conformità alle presenti Norme oppure (ii) il Team Privacy richieda un audit specifico (ad hoc).

2.2.2 Analogamente, l'ambito e la copertura dell'audit saranno stabiliti dalla funzione di Audit interno sulla base di un'analisi dei rischi effettuata secondo la metodologia approvata.

2.2.3 Tutti gli aspetti delle presenti Norme (ad es., applicazioni, sistemi informatici, trasferimenti successivi, ecc.), compresi i metodi e i piani d'azione volti a garantire l'attuazione delle azioni correttive, saranno esaminati secondo un approccio basato sul rischio, al fine di determinare l'ambito specifico dell'audit; tale esame sarà effettuato, come sopra indicato, a intervalli regolari adeguati.

2.3 Auditor

2.3.1 Gli audit previsti dal presente documento saranno effettuati da auditor interni della funzione di Audit interno o, a seconda dei casi, da auditor esterni accreditati. Qualora gli audit siano svolti da auditor esterni, dovranno essere soddisfatte le seguenti condizioni:

(a) Svolgere un'adeguata procedura di due diligence prima della loro selezione, al fine di garantire che gli auditor interessati possiedano qualifiche e requisiti adeguati per collaborare allo svolgimento di tale attività; e

(b) Stipulare con gli stessi un accordo che disciplini la prestazione dei loro servizi conformemente alla normativa applicabile.

2.4 Indipendenza

2.4.1 Alle persone incaricate di decidere in merito al Programma di audit o di svolgere gli audit è garantita l'indipendenza nell'esercizio delle proprie funzioni.

2.5 Relazione

2.5.1 Al termine dell'audit, in funzione della natura dello stesso, la relazione e le relative risultanze saranno messe a disposizione dell'alta dirigenza, dell'Ufficio DP centrale e dell'RPD o del referente per la protezione dei dati e saranno comunicate al Comitato per il controllo interno del Consiglio di amministrazione e al Consiglio di amministrazione del Membro responsabile per le violazioni. La relazione di audit conterrà inoltre informazioni dettagliate sulle eventuali azioni correttive necessarie, sulle raccomandazioni e sui termini previsti per l'attuazione di tali azioni.

2.5.2 I Membri del Gruppo hanno convenuto di fornire, su richiesta, una copia dei risultati di qualsiasi audit relativo alle presenti Norme a ogni autorità di controllo competente.

2.5.3 L'RPD o il referente per la protezione dei dati avrà la responsabilità di interagire con le autorità di controllo competenti ai fini della trasmissione delle informazioni sopra indicate.

APPENDICE 2

PROCEDURA DI GESTIONE DEI RECLAMI

1. INTRODUZIONE

1.1 La presente Procedura di gestione dei reclami ha lo scopo di illustrare le modalità di gestione dei reclami presentati da un interessato i cui dati personali siano trattati dai Membri del Gruppo ai sensi delle presenti Norme.

2. MODALITÀ DI PRESENTAZIONE DEI RECLAMI DA PARTE DEGLI INTERESSATI

Tutti i reclami degli interessati i cui dati personali siano trattati conformemente alle presenti Norme possono essere presentati per iscritto, anche tramite e-mail, all'RPD o al referente per la protezione dei dati, a seconda dei casi. Gli interessati possono presentare un reclamo utilizzando i seguenti recapiti:

Alla cortese attenzione del: Team Privacy

Indirizzo: [inserire l'indirizzo postale]

E-mail: L'elenco degli indirizzi e-mail pertinenti è disponibile qui.

In ogni caso, saranno gestiti anche i reclami presentati con qualsiasi altro mezzo, purché siano debitamente comunicati al Membro del Gruppo competente.

3. CHI GESTISCE I RECLAMI?

3.1 L'RPD o il referente per la protezione dei dati, a seconda dei casi, gestirà tutti i reclami presentati ai sensi delle presenti Norme in relazione al trattamento dei dati personali. L'RPD o il referente per la protezione dei dati, a seconda dei casi, collaborerà con le unità aziendali interessate per esaminare il reclamo e coordinerà la risposta, che dovrà comprendere informazioni sulle azioni intraprese e sarà trasmessa al reclamante.

3.2 Quali sono i tempi di risposta?

L'RPD o il referente per la protezione dei dati, con il supporto del Team Privacy, confermerà all'interessato la ricezione del reclamo entro dieci giorni lavorativi; successivamente svolgerà le opportune verifiche e fornirà una risposta nel merito, contenente informazioni sulle azioni intraprese, senza ingiustificato ritardo e, in ogni caso, entro un mese di calendario. Qualora, a causa della complessità del reclamo o del numero di richieste, non sia possibile fornire una risposta nel merito entro tale termine, l'RPD o il referente per la protezione dei dati, con il supporto del Team Privacy, informerà il reclamante dei motivi del ritardo entro un mese di calendario dalla ricezione del reclamo e gli comunicherà un termine ragionevolmente stimato per la risposta, che non potrà superare ulteriori due mesi di calendario dalla data in cui l'interessato è stato informato della proroga.

Qualora il termine di risposta non sia rispettato e la risposta al reclamo subisca un ritardo senza che ne siano stati comunicati i motivi, l'interessato potrà segnalarlo all'RPD o al referente per la protezione dei dati, il quale, senza ingiustificato ritardo e, in ogni caso, entro dieci giorni di calendario, spiegherà le ragioni del ritardo e informerà l'interessato delle azioni intraprese fino a quel momento. La questione sarà sottoposta all'Ufficio DP centrale, unitamente a una relazione motivata che individui

le misure da adottare. L'Ufficio riesaminerà il caso e indicherà all'RPD o al referente per la protezione dei dati come risolvere quanto contestato nel reclamo nel più breve tempo possibile. In ogni caso, l'interessato potrà inoltre esercitare i diritti descritti al punto 3.4 della presente Appendice 2.

3.3 Contestazione delle conclusioni o del rigetto di un reclamo

Qualora un reclamo sia ritenuto fondato, l'RPD o il referente per la protezione dei dati adotterà le misure necessarie per risolvere la questione sollevata dall'interessato e ne informerà quest'ultimo.

Qualora il reclamante contesti la risposta dell'RPD o del referente per la protezione dei dati, compreso l'eventuale rifiuto di esaminare o accogliere il reclamo, oppure qualsiasi aspetto delle conclusioni, potrà comunicarlo all'RPD o al referente per la protezione dei dati. La questione sarà sottoposta all'Ufficio DP centrale, che riesaminerà il caso e, tramite l'RPD o il referente per la protezione dei dati della società del Gruppo comunicherà al reclamante la decisione definitiva di confermare le conclusioni originarie o di sostituirle con nuove conclusioni. L'Ufficio DP locale competente risponderà al reclamante entro un mese di calendario dal deferimento della questione. Qualora, a causa della complessità del reclamo, non sia possibile fornire una risposta nel merito entro tale termine, l'Ufficio DP centrale informerà il reclamante del motivo del ritardo entro un mese di calendario dalla ricezione del deferimento e gli comunicherà un termine ragionevolmente stimato per la risposta, che non potrà superare ulteriori due mesi di calendario. Se il reclamo viene accolto, l'Ufficio DP centrale provvederà, di conseguenza, affinché siano adottate tutte le misure necessarie.

3.4 Meccanismi alternativi di reclamo

Gli interessati i cui dati personali siano trattati conformemente alle presenti Norme hanno inoltre il diritto di: (i) presentare reclamo all'autorità di controllo dello Stato membro nel quale si è verificata la presunta violazione o nel quale l'interessato lavora abitualmente o risiede; e/o (ii) agire dinanzi all'autorità giudiziaria competente del Paese europeo nel quale è stabilito il Membro del Gruppo o del Paese europeo nel quale risiede l'interessato. Come ulteriormente precisato ai punti da C.2 a C.4, qualora una violazione sia commessa da un Membro del Gruppo situato al di fuori del SEE, gli interessati conserveranno il diritto di presentare reclamo e agire in giudizio nei confronti del Membro responsabile per le violazioni designato, come se la violazione fosse stata commessa da tale soggetto nello Stato membro in cui è stabilito. Tali diritti si applicheranno indipendentemente dal fatto che gli interessati abbiano previamente presentato un reclamo a un Membro del Gruppo mediante la presente Procedura di gestione dei reclami.

APPENDICE 3

PROCEDURA DI COOPERAZIONE

1. PROCEDURA DI COOPERAZIONE

1.1 La presente Procedura di cooperazione stabilisce le modalità con cui i Membri del Gruppo coopereranno con le autorità di controllo competenti e accetteranno di essere sottoposti ad audit e ispezioni da parte delle stesse, anche in loco ove necessario, in relazione alle presenti Norme, nonché di tenere conto delle loro indicazioni e rispettare le loro decisioni in merito a qualsiasi questione relativa alle presenti Norme.

1.2 Ove richiesto, i Membri del Gruppo metteranno il personale competente a disposizione dell'autorità di controllo competente per interloquire in merito alle presenti Norme.

1.3 Su richiesta, l'RPD, il referente per la protezione dei dati o la funzione di audit interno competente, a seconda dei casi, fornirà a qualsiasi autorità di controllo competente una copia dei risultati di qualsiasi audit relativo alle presenti Norme effettuato ai sensi dell'Appendice 1, nonché tutte le informazioni sulle operazioni di trattamento contemplate dalle presenti Norme. Al momento della ricezione di tali informazioni, all'autorità sarà ricordato il proprio obbligo di segreto professionale.

1.4 I Membri del Gruppo convengono che le autorità di controllo competenti possano sottoporli a un audit o a un'ispezione in materia di protezione dei dati, anche in loco ove necessario, conformemente alla normativa europea sulla protezione dei dati applicabile all'Esportatore interessato.

1.5 Tutti i Membri del Gruppo accettano di essere sottoposti ad audit da parte delle autorità di controllo competenti conformemente alle procedure di audit applicabili di tali autorità.

1.6 I Membri del Gruppo convengono che qualsiasi controversia relativa all'esercizio, da parte di un'autorità di controllo competente, dei poteri di controllo sulle presenti Norme sarà risolta dagli organi giurisdizionali dello Stato membro in cui ha sede tale autorità, conformemente al diritto processuale di detto Stato membro.

APPENDICE 4

PROCEDURA DI AGGIORNAMENTO

1. INTRODUZIONE E PRINCIPI GENERALI

1.1 La presente Procedura di aggiornamento stabilisce le modalità con cui le modifiche alle presenti Norme saranno comunicate alle autorità di controllo competenti, agli interessati e ai Membri del Gruppo vincolati dalle Norme.

1.2 Le presenti Norme saranno mantenute aggiornate al fine di riflettere la situazione e il contesto attuali in materia di protezione dei dati personali.

2. MODIFICHE SOSTANZIALI ALLE NORME

2.1 L'RPD di Banco Santander e la funzione legale centrale comunicheranno preventivamente all'Agenzia spagnola per la protezione dei dati (l'"**autorità capofila per le norme vincolanti d'impresa**") e, tramite quest'ultima, alle autorità di controllo competenti qualsiasi modifica sostanziale alle presenti Norme (ossia qualsiasi modifica che possa pregiudicare il livello di protezione offerto dalle Norme o incidere significativamente sulle stesse, ad esempio modificandone il carattere vincolante).Tale comunicazione comprenderà una breve spiegazione dei motivi dell'aggiornamento. L'autorità di controllo competente valuterà inoltre se le modifiche apportate richiedano una nuova approvazione.

3. ALTRE MODIFICHE ALLE NORME

3.1 L'RPD di Banco Santander e la funzione legale centrale comunicheranno all'autorità capofila per le norme vincolanti d'impresa e, tramite quest'ultima, alle altre autorità di controllo interessate, su richiesta e almeno una volta all'anno, le modifiche apportate alle presenti Norme o l'assenza di modifiche. Tale aggiornamento annuale comprenderà inoltre il rinnovo della conferma che il Membro responsabile per le violazioni dispone di risorse finanziarie sufficienti o ha adottato misure adeguate che gli consentano di corrispondere il risarcimento dei danni derivanti da una violazione delle presenti Norme.

3.2 Esempi delle suddette modifiche possono includere modifiche di natura amministrativa (compresi gli aggiornamenti dell'elenco dei Membri del Gruppo), modifiche intervenute a seguito di una variazione della normativa europea applicabile in materia di protezione dei dati oppure modifiche derivanti da provvedimenti legislativi, decisioni giudiziarie o misure e orientamenti delle autorità di controllo (compresi gli orientamenti del Comitato europeo per la protezione dei dati). Banco Santander fornirà inoltre all'autorità capofila per le norme vincolanti d'impresa e alle altre autorità di controllo una breve spiegazione dei motivi delle modifiche apportate alle Norme oggetto di comunicazione.

4. NUOVI MEMBRI DEL GRUPPO

4.1 Gli RPD e i referenti per la protezione dei dati, insieme al Team Privacy, garantiranno che tutti i nuovi Membri del Gruppo siano effettivamente vincolati dalle presenti Norme e siano in grado di garantirne la conformità prima di effettuare qualsiasi trasferimento di dati personali a tali Membri.

5. COMUNICAZIONE E REGISTRAZIONE DELLE MODIFICHE ALLE NORME

5.1 Le presenti Norme contengono un registro delle modifiche in cui sono riportate le date delle revisioni e le informazioni dettagliate su ciascuna modifica apportata. La funzione legale centrale manterrà aggiornato l'elenco delle modifiche apportate alle presenti Norme, mentre l'Ufficio DP centrale manterrà aggiornato l'elenco dei Membri del Gruppo vincolati dalle stesse.

5.2 La funzione legale centrale, con il supporto dell'Ufficio DP centrale, comunicherà tutte le modifiche alle presenti Norme, siano esse sostanziali o di altra natura:

(a) senza ingiustificato ritardo, ai Membri del Gruppo vincolati dalle presenti Norme e pubblicherà una versione aggiornata delle stesse sulla rete interna del Gruppo Santander;

(b) sistematicamente agli interessati che beneficiano delle presenti Norme, tramite il sito web della società (Sito web di Santander); e

(c) su richiesta e tramite gli RPD locali competenti (o figure analoghe), all'autorità di controllo competente.