

## American Express - Norme vincolanti di impresa UE (BCR UE)

### Indice

1. Introduzione
2. Natura vincolante delle BCR
3. Ambito di applicazione delle nostre BCR
4. In che modo American Express protegge i vostri Dati Personalii?
5. Rete DPO di American Express
6. Formazione e Consapevolezza
7. Audit e Controlli
8. Conformità, Esecuzione e Responsabilità
9. Come proporre reclamo e far rispettare le BCR UE
10. Obbligo di collaborazione con le Autorità di controllo
11. Come gestire potenziali conflitti normativi e affrontare le richieste di accesso da parte delle autorità governative?
12. Non conformità alle BCR UE
13. Cessazione
14. Aggiornamenti alle BCR UE

Appendice 1 - Natura e finalità dei Trasferimenti di Dati personali nell'ambito delle BCR  
UE

Appendice 2 - Ubicazione delle Società del gruppo American Express vincolate alle BCR

### Glossario

#### 1. INTRODUZIONE

##### 1.1. Overview

American Express attribuisce grande valore alla fiducia accordatale e considera prioritario il rispetto della privacy.

La protezione dei dati e la sicurezza delle informazioni rappresentano da sempre una priorità per la nostra società. Infatti, in quanto società multinazionale, siamo impegnati nella protezione dei dati personali, indipendentemente dal loro contesto di utilizzo, e garantiamo che tutti i dati personali raccolti siano trattati secondo i nostri [Principi di privacy e protezione dei dati](#).

Nel 2012 American Express è stata tra le prime società a pubblicare le Binding Corporate Rules (BCR - Norme vincolanti d'impresa), approvate dall'ICO (Information

Commissioner's Office), che ancora oggi continuano a rappresentare la base del nostro forte impegno in materia di privacy, promuovendo una solida cultura della compliance in tutta la nostra organizzazione aziendale.

Le nostre BCR disciplinano diversi aspetti, tra cui i Trasferimenti internazionali di Dati personali nell'ambito delle Società del gruppo American Express vincolate alle BCR in conformità alla normativa applicabile in materia di protezione dei dati, e garantiscono che i Dati personali degli Interessati siano sempre opportunamente protetti indipendentemente dal luogo in cui vengono trasferiti.

## 1.2. Accesso alle BCR

Le nostre BCR possono essere facilmente consultate dagli Interessati sui siti web di American Express in tutta Europa. Gli Interessati possono inoltre richiedere una copia delle nostre BCR in un formato alternativo al nostro Responsabile della protezione dei dati ("DPO") all'indirizzo indicato di seguito o alle Società del gruppo American Express vincolate alle BCR responsabile dei propri Dati personali. L'Autorità di controllo capofila incaricata della supervisione delle nostre BCR è l'Agencia Española de Protección de Datos (AEPD) ("Autorità di controllo capofila").

## 2. NATURA VINCOLANTE DELLE BCR

Le nostre BCR sono legalmente vincolanti per le Società parte del Gruppo American Express e per i loro Dipendenti, in applicazione di un Accordo infragruppo stipulato tra American Express Company e AEESA, rappresentante legale di American Express nello Spazio economico europeo (di seguito, SEE). AEESA è la società europea di American Express che ha assunto la responsabilità di garantire che i Dati personali siano trattati in conformità alle BCR.

Tutte le Società del gruppo American Express vincolate alle BCR e i relativi Dipendenti sono autorizzati al Trattamento dei Dati Personalni solo entro il perimetro previsto dalle presenti BCR e in conformità alle stesse. In caso di violazione delle BCR da parte dei Dipendenti potranno essere intraprese azioni disciplinari.

## 3. AMBITO DI APPLICAZIONE DELLE NOSTRE BCR

### 3.1. Ambito geografico

Le BCR di American Express si applicano a tutte le attività di trattamento da parte delle Società del gruppo American Express che rientrano nel perimetro previsto dalle BCR, relative a Dati personali soggetti alla Normativa applicabile in materia di protezione dei dati, come indicato di seguito:

- (a) Dati personali degli Interessati trasferiti da una Società del gruppo American Express vincolata alle BCR ad una Società del gruppo American Express vincolata alle BCR situata in un Paese terzo; e
- (b) Dati personali degli Interessati soggetti a Trasferimenti successivi ad altre Società del gruppo American Express vincolate alle BCR situate in un Paese terzo.

Il gruppo American Express comprende diverse persone giuridiche dislocate in tutto il mondo. La società controllante del gruppo è la persona giuridica American Express Company. AEESA e le altre Società del gruppo American Express vincolate alle BCR sono direttamente o indirettamente di proprietà di American Express Company.

Nell'allegato 2 è riportato l'elenco delle Società del gruppo American Express vincolate alle norme BCR.

### 3.2. Ambito di applicazione materiale

Le BCR American Express si applicano al Trattamento dei Dati personali descritto in questa sezione.

In qualità di Titolare del trattamento, American Express tratta i Dati personali di dipendenti, amministratori, appaltatori, consulenti e collaboratori occasionali assunti o incaricati da American Express, che siano cessati, in carica o potenziali, full time o part time, a tempo determinato o indeterminato, anche se in pensione ("Dipendenti"), e i Dati personali dei clienti passati, presenti e potenziali di American Express e delle persone fisiche che lavorano presso aziende clienti, fornitori e partner di American Express ("Clienti").

Le finalità per cui American Express tratta Dati personali riguardano principalmente i servizi commerciali, d'affari e assicurativi, servizi relativi a viaggi, riunioni ed eventi, servizi di rete e ai consumatori, nonché le risorse umane.

Per una gestione efficace delle attività globali di American Express, il Trattamento dei Dati personali da parte delle Società del gruppo American Express vincolate alle BCR nell'ambito delle finalità identificate nelle presenti BCR potrebbe implicare Trasferimenti internazionali di Dati personali degli Interessati, da qualsiasi Società del gruppo American Express vincolata alle BCR soggetta al GDPR a qualsiasi altra Società del gruppo American Express vincolata alle BCR in un Paese terzo (compresi Trasferimenti da Paesi all'interno dello SEE verso gli Stati Uniti, dove sono ubicati i server principali di American Express), e qualsiasi altro Trasferimento successivo verso Società del gruppo American Express vincolate alle BCR in un Paese terzo.

Per una panoramica più completa delle attività di Trattamento di American Express si rimanda all'Allegato 1. Per conoscere l'ubicazione delle nostre Società del gruppo American Express vincolate alle BCR si rimanda all'Allegato 2.

#### 4. IN CHE MODO AMERICAN EXPRESS PROTEGGE I VOSTRI DATI PERSONALI?

Nel corso del Trattamento dei Dati personali degli Interessati, le Società del gruppo American Express vincolate alle BCR si impegnano a rispettare rigorosi principi di protezione dei dati (sezione 4.1) e i diritti degli Interessati in materia di protezione dei dati (sezione 4.2).

##### 4.1. Principi di protezione dei dati

###### 4.1.1. Trasparenza e correttezza

Le Società del gruppo American Express vincolate alle BCR raccolgono e trattano i Dati personali degli Interessati in modo corretto e trasparente.

American Express si assicura che gli Interessati possano accedere con facilità alle informazioni relative alle attività di Trattamento svolte, come richiesto dal GDPR. Tali informazioni vengono fornite agli Interessati in forma concisa, trasparente, comprensibile e facilmente accessibile, con un linguaggio semplice e chiaro, come da Informativa sulla Privacy di American Express applicabile al rapporto che intercorre tra l'Interessato e American Express. Tale Informativa e i Termini e condizioni possono inoltre contenere ulteriori disposizioni relative al Trattamento dei Dati personali ai sensi della legge nazionale e locale applicabile (o delle leggi nazionali e locali applicabili) alla Società del gruppo American Express vincolata alle BCR di riferimento.

In particolare, qualora i Dati personali siano raccolti presso l'Interessato saranno contestualmente fornite le seguenti informazioni:

- identità e dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante;
- dati di contatto del DPO;
- finalità del Trattamento cui sono destinati i Dati personali, nonché la base giuridica del Trattamento, inclusa una spiegazione dei legittimi interessi perseguiti, ove applicabile;
- eventuali destinatari o categorie di destinatari dei Dati personali;

- eventuali Trasferimenti dei Dati personali, oltre a informazioni relative alle adeguate garanzie adottate per assicurare lo stesso livello di protezione richiesto dal GDPR e alle modalità di accesso o rilascio di una copia di tali garanzie. In caso di Trasferimenti di Dati personali tra un Esportatore di dati e un Importatore di dati nell'ambito delle presenti BCR, le informazioni fornite includeranno un riferimento alle presenti BCR e alle relative modalità di accesso;
- periodo di conservazione dei Dati personali o, se ciò non fosse possibile, criteri utilizzati per determinare tale periodo;
- eventuali diritti degli Interessati riconosciuti dal GDPR e modalità di esercizio di tali diritti;
- se la comunicazione di dati personali è un obbligo legale o contrattuale nonché le possibili conseguenze della mancata comunicazione di tali Dati personali in simili circostanze; e
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione; almeno nei casi in cui tali decisioni producono effetti giuridici sugli Interessati o incidano in modo analogo e considerevole sugli Interessati, o qualora siano basate su Categorie particolari di dati, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per gli Interessati.

Qualora i Dati personali non siano stati ottenuti presso l'Interessato, le informazioni precedenti, le categorie di Dati personali in questione e la fonte da cui hanno origine tali Dati personali saranno comunicate tempestivamente e in conformità ai tempi previsti dalla Normativa applicabile in materia di protezione dei dati (tali indicazioni non si applicano se: l'Interessato dispone già di tali informazioni; comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro; i Dati personali devono rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge).

Inoltre, le BCR American Express: (a) informano gli Interessati relativamente ai diritti che hanno la facoltà di esercitare nei confronti di AEESA o di qualsiasi Società del gruppo American Express vincolata alle BCR in qualità di terzo beneficiario per quanto riguarda il Trattamento dei propri Dati personali nell'ambito delle presenti BCR ("Diritti del terzo beneficiario") e in merito alle modalità di esercizio di tali diritti (cfr. sezione 8); (b) forniscono agli Interessati una panoramica dell'ambito di applicazione delle BCR; (c) forniscono agli Interessati informazioni relative ai principi di protezione dei dati

che American Express applica al Trattamento dei Dati personali (come specificato nella presente sezione 4); e (d) forniscono agli Interessati informazioni relative alla responsabilità assunta dalle Società del gruppo American Express vincolate alle BCR in caso di violazione delle presenti BCR (cfr. sezione 8).

Inoltre, l'Interessato ha la facoltà, in ogni momento, di richiedere e ottenere una copia delle BCR American Express. Le nostre BCR sono disponibili sui siti web pubblici delle Società del gruppo American Express vincolate alle BCR in tutto lo SEE e sulla nostra intranet se l'Interessato è un Dipendente.

#### 4.1.2. Liceità del trattamento

I Dati personali degli Interessati e le Categorie particolari di dati vengono raccolti e trattati in modo corretto e lecito, in conformità alla Normativa applicabile in materia di protezione dei dati. I fondamenti giuridici del Trattamento dei Dati personali degli Interessati sono descritti nel dettaglio nell'Informativa sulla Privacy di American Express applicabile al rapporto che intercorre tra l'Interessato e American Express.

- Trattamento dei Dati personali

I Dati personali degli Interessati sono raccolti e trattati solo in presenza di una base giuridica del Trattamento, compresi i casi in cui:

- l'Interessato ha espresso il Consenso al Trattamento dei propri Dati personali (es. per l'invio di comunicazioni tramite e-mail contenenti annunci, promozioni e offerte di prodotti e servizi American Express);
- il Trattamento è necessario per l'esecuzione di un contratto di cui l'Interessato è parte o per l'esecuzione di misure precontrattuali adottate su richiesta dello stesso (es. per la gestione del rapporto contrattuale in essere tra l'Interessato e American Express e per poter evadere una richiesta dell'Interessato relativa a una carta, un conto o un altro prodotto, o per gestire i conti già esistenti a suo nome);
- il Trattamento è necessario per adempiere un obbligo legale (es. per la segnalazione di particolari transazioni sospette alle Autorità competenti ai sensi delle norme antiriciclaggio o, come previsto dalla legge, per svolgere attività di due diligence dei Clienti prima di approvarne le richieste);
- il Trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica (es. per l'eventuale necessità di trattare i dati di un Dipendente in caso di emergenza medica);

- il Trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento (es. a fini fiscali, ove previsto dal diritto dello Stato membro cui è soggetto il Titolare del trattamento); oppure

- il Trattamento è necessario per il perseguimento del legittimo interesse di una Società del gruppo American Express vincolata alle BCR o di terzi (es. per fornire prodotti o erogare servizi, pubblicizzare e commercializzare prodotti e servizi, condurre ricerche e analisi e gestire i rischi di frode e sicurezza cui è soggetta American Express - a titolo esemplificativo, la condivisione di informazioni ritenute sospette tra due diverse entità con l'obiettivo di contattare il Cliente e verificarle), a condizione che tale interesse non prevalga sugli interessi o diritti e libertà fondamentali dell'Interessato.

- Trattamento di Categorie particolari di dati

American Express ha la facoltà di raccogliere Categorie particolari di dati.

Tali dati vengono raccolti e trattati solo se necessario per le finalità del Trattamento. Nella misura limitata in cui vengono raccolte Categorie particolari di dati, il Trattamento sarà condotto unicamente nell'ambito di una delle basi giuridiche sopra menzionate e solo se si applica una delle condizioni per il Trattamento di Categorie particolari di dati indicate di seguito:

- L'Interessato ha prestato il proprio consenso esplicito al Trattamento di tali Dati personali per una o più finalità specifiche, salvo nei casi in cui la Normativa applicabile in materia di protezione dei dati dispone che l'Interessato non possa revocare il divieto di Trattamento di tali Categorie particolari di dati;
- il Trattamento è necessario per tutelare un interesse vitale dell'Interessato o di un'altra persona fisica qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il Trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il Trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i Dati personali non siano comunicati all'esterno senza il consenso dell'Interessato;
- il Trattamento riguarda Categorie particolari di dati resi manifestamente pubblici dall'Interessato;

- il Trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria oognqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il Trattamento è necessario per motivi di interesse pubblico rilevante sulla base della Normativa applicabile in materia di protezione dei dati, e deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla Protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato;
- il Trattamento è necessario 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 sulla base della Normativa applicabile in materia di protezione dei dati o conformemente al contratto con un professionista della sanità, a condizione che tali Dati personali vengano trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente alla Normativa applicabile in materia di protezione dei dati o alle norme stabilite dagli organismi nazionali competenti;
- il Trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base della Normativa applicabile in materia di protezione dei dati che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'Interessato, in particolare il segreto professionale;
- il Trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici sulla base della Normativa applicabile in materia di protezione dei dati; il Trattamento deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato;
- l'Interessato è un Dipendente e il Trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici di American Express o dell'Interessato in materia di diritto del lavoro e di assistenza e previdenza sociale, nella misura in cui sia autorizzato dalla Normativa applicabile in materia di protezione dei dati o da un contratto collettivo ai sensi della Normativa applicabile in materia di protezione dei dati, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'Interessato;

Per quanto riguarda il Trattamento dei Dati personali relativi a condanne penali e reati o a connesse misure di sicurezza, le Società del gruppo American Express vincolate alle BCR procederanno con tale Trattamento soltanto sotto il controllo dell'autorità pubblica o se il Trattamento è autorizzato dalle leggi che prevedono garanzie appropriate per i diritti e le libertà degli Interessati in conformità ai fondamenti giuridici di cui sopra.

Inoltre, in considerazione del maggiore grado di protezione riservato alle Categorie particolari di dati ai sensi della Normativa applicabile in materia di protezione dei dati, le Società del gruppo American Express vincolate alle BCR adotteranno misure potenziate per il Trattamento delle Categorie particolari di dati, come previsto dalla Normativa applicabile sulla protezione dei dati.

#### 4.1.3. Minimizzazione dei dati, accuratezza e limitazione della conservazione

Le Società del gruppo American Express vincolate alle BCR utilizzano tecnologie appropriate e prassi consolidate tra i Dipendenti per il Trattamento dei Dati personali dell'Interessato in modo tempestivo ed esatto.

American Express adotta misure ragionevoli per garantire che i Dati personali dell'Interessato siano:

- Esatti e, se necessario, aggiornati rispetto alle finalità per le quali sono trattati (accuratezza dei dati). I Dati personali inesatti vengono cancellati o rettificati tempestivamente. Abbiamo adottato specifiche misure per garantire che i Dati personali errati vengano cancellati, corretti, integrati o rettificati (secondo necessità). Ad esempio, i nostri Responsabili del trattamento sono contrattualmente vincolati a collaborare e ad assisterci nell'adempimento di questo requisito, ai sensi della Normativa applicabile in materia di protezione dei dati. Inoltre, abbiamo implementato specifiche policy che stabiliscono gli standard a cui le Società del gruppo American Express vincolate alle BCR devono conformarsi;
- Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali i Dati personali sono raccolti e trattati (minimizzazione dei dati). In particolare, questo requisito viene tenuto in considerazione nella fase di raccolta iniziale dei dati degli Interessati (es. nel modulo di richiesta per i titolari di carta di credito) per garantire che sia limitata alla quantità minima di Dati personali necessaria per la finalità in questione;
- Conservati in formato identificabile solo per il tempo necessario per le finalità per le quali i Dati personali sono trattati e non oltre, e conservati per un periodo più lungo solo a fini di archiviazione o come altrimenti consentito o previsto in conformità alle leggi applicabili (es. legge locale della Società del gruppo American Express vincolata alle BCR di riferimento situata in un Paese terzo) e solo se

vengono adottate misure amministrative, tecniche e organizzative appropriate. Abbiamo implementato un framework di conservazione dei dati all'interno di American Express che stabilisce tempi appropriati per le registrazioni dei dati e la loro conservazione, e policy che definiscono gli standard a cui le Società del gruppo American Express vincolate alle BCR devono conformarsi.

#### 4.1.4. Limitazione della finalità

Le Società del gruppo American Express vincolate alle BCR raccolgono Dati personali solo per finalità specifiche e legittime. American Express tratta i Dati personali dell'Interessato in modo corretto e solo per le finalità che sono state comunicate all'Interessato, che siano state autorizzate dall'Interessato stesso o dalla Normativa applicabile in materia di protezione dei dati. Garantiamo la conformità a questo principio in diversi modi, che comprendono l'inclusione degli standard di privacy e protezione dei dati nel nostro processo di approvazione dei nuovi prodotti.

American Express garantirà che i Dati personali dell'Interessato non siano sottoposti a ulteriori Trattamenti in un modo che sia incompatibile con tali finalità.

#### 4.1.5. Sicurezza e riservatezza dei dati

American Express opera in un settore soggetto a numerose e stringenti disposizioni normative e le autorità di regolamentazione impongono elevati e rigorosi standard per quanto riguarda le procedure nell'ambito della sicurezza delle informazioni e della privacy. American Express ha implementato e si impegna a mantenere un programma completo in forma scritta relativo alla sicurezza delle informazioni, conforme alle leggi applicabili (comprese quelle che possono essere applicabili ad una Società del gruppo American Express vincolata alle BCR situata in un Paese terzo) e alla Normativa applicabile in materia di protezione dei dati.

Le Società del gruppo American Express vincolate alle BCR adottano misure amministrative, tecniche e organizzative appropriate per proteggere i Dati personali dell'Interessato da rischi quali la distruzione accidentale o illegale, la perdita, la modifica, la divulgazione o l'accesso non autorizzato a Dati personali trasmessi, conservati o comunque trattati. American Express garantirà la riservatezza dei Dati personali dell'Interessato e limiterà l'accesso a tali Dati personali a coloro che ne hanno specificamente necessità nello svolgimento delle proprie attività professionali, salvo se diversamente previsto dalla legge applicabile ad American Express.

Tali misure garantiscono un livello di sicurezza appropriato al rischio e tengono in considerazione lo stato dell'arte, i costi di implementazione e la natura, l'ambito, il contesto e le finalità del Trattamento, nonché il rischio di variazioni in termini di

probabilità e gravità per i diritti e le libertà degli Interessati, e possono includere, a seconda dei casi:

- la pseudonimizzazione e la cifratura dei Dati personali (es. come, ove appropriato, la tokenizzazione e i controlli di gestione degli accessi);
- misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (es. standard crittografici e policy volte a supportare e disciplinare le nostre procedure);
- misure per garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai Dati personali in caso di incidente fisico o tecnico; e
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento.

American Express richiede inoltre che vengano adottate dai terzi autorizzati misure amministrative, tecniche e organizzative appropriate al Trattamento dei Dati personali degli Interessati per nostro conto (che possono includere le misure precedentemente indicate, a seconda dei casi) e assume impegni contrattuali con Responsabili del trattamento interni ed esterni in conformità alle garanzie previste dal GDPR.

In particolare, il Trattamento da parte di un Responsabile del trattamento (sia interno al gruppo American Express sia esterno) dovrà essere disciplinato da un contratto che vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del Trattamento, la natura e le finalità del Trattamento, il tipo di Dati personali e le categorie di Interessati, gli obblighi e i diritti del Titolare del trattamento.

Il contratto dovrà prevedere, in particolare, che il Responsabile del trattamento:

- tratti i Dati Personalni soltanto su istruzione documentata del Responsabile del trattamento, anche in caso di Trasferimento di Dati Personalni, salvo che lo richieda una legislazione cui è soggetto il Responsabile del trattamento (in tal caso, il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vietи tale informazione per rilevanti motivi di interesse pubblico);
- garantisca che le persone autorizzate al Trattamento dei Dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

- adotti tutte le misure tecniche e organizzative necessarie per garantire un livello di sicurezza appropriato e adeguato al rischio connesso al Trattamento dei Dati personali;
- non ricorra ad un altro Responsabile del trattamento ("Sub-responsabile"), senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento e solo a condizione che su tale altro Sub-responsabile siano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel contratto tra il Titolare del trattamento e il Responsabile del trattamento (prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti della Normativa applicabile in materia di protezione dei dati);
- tenendo conto della natura del Trattamento, assista il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'Interessato;
- assista il Titolare del trattamento nel garantire il rispetto dei suoi obblighi in materia di sicurezza del Trattamento, Violazione dei dati personali e Valutazione d'impatto sulla protezione dei dati (compreso il caso in cui sia richiesta la consultazione con un'Autorità di controllo competente in relazione ad una Valutazione d'impatto sulla protezione dei dati);
- su scelta del Titolare del trattamento, cancelli o restituisca tutti i Dati personali al Titolare del trattamento al termine della prestazione dei servizi relativi al Trattamento, e cancelli le copie esistenti, salvo che la legge applicabile (es. legge locale della Società del gruppo American Express vincolata alle BCR di riferimento situata al di fuori dello SEE) preveda la conservazione dei Dati personali;
- metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del Responsabile del trattamento di cui all'articolo 28 del GDPR e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato; e
- informi immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione del Titolare del trattamento violi la Normativa applicabile in materia di protezione dei dati.

Inoltre, le Società del gruppo American Express vincolate alle BCR hanno adottato misure amministrative, tecniche e organizzative per individuare, esaminare, fare escalation e rimediare alle Violazioni di dati personali.

AEESA e il DPO di American Express ricevono comunicazione di eventuali Violazioni di dati personali da parte della Società del gruppo American Express vincolata alle BCR di riferimento senza ingiustificato ritardo. Se una Società del gruppo American Express vincolata alle BCR agisce in qualità di Responsabile del trattamento per conto di un'altra Società del gruppo American Express vincolata alle BCR (in qualità di Titolare del trattamento), il Responsabile del trattamento dovrà informare tale Titolare del trattamento senza ingiustificato ritardo.

Il DPO di American Express determinerà se notificare tale violazione: (a) all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (a meno che sia improbabile che la Violazione dei dati personali presenti un rischio per i diritti e le libertà degli Interessati); e (b) all'Interessato qualora tale violazione presenti un potenziale rischio elevato per i suoi diritti e le sue libertà, in entrambi i casi in conformità ai requisiti del GDPR.

Qualsiasi Violazione dei dati personali viene documentata (comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio) e tale documentazione viene messa a disposizione dell'Autorità di controllo competente su richiesta.

#### 4.1.6. Trasferimenti successivi

I Dati personali dell'Interessato vengono trasferiti tra le Società del gruppo American Express vincolate alle BCR e successivamente a terze parti, garantendo sempre un livello di protezione adeguato al Trattamento dei Dati dell'Interessato come previsto dalla Normativa applicabile in materia di protezione dei dati, indipendentemente dal luogo in cui vengono trasferiti.

Questo flusso di dati è legittimato dalle nostre BCR, che consentono ad American Express di trasferire Dati personali dal SEE alle Società del gruppo American Express vincolate alle BCR situate in Paesi terzi.

In tutti i casi di Trasferimenti successivi (vale a dire Dati personali che sono stati precedentemente trasferiti da una Società del gruppo American Express vincolata alle BCR a un'altra Società del gruppo American Express vincolata alle BCR non SEE e successivamente trasferiti a terzi non soggetti alle BCR), le Società del gruppo American Express vincolate alle BCR garantiranno quanto segue:

- (a) verrà stipulato un contratto in forma scritta con queste terze parti contenente disposizioni volte ad assicurare che i Dati personali siano protetti in misura almeno pari agli standard di riservatezza e sicurezza previsti dalle presenti BCR (qualora tale terza parte sia un Responsabile del trattamento, il contratto

riporterà anche i doveri del Responsabile del trattamento di cui alla sezione 4.1.5 delle presenti BCR); e

- (b) in mancanza di una decisione di adeguatezza, verrà prevista una garanzia appropriata per assicurare che il Trasferimento sia legittimo e che siano fornite garanzie adeguate ai sensi dell'articolo 46 del GDPR.

In mancanza di una decisione di adeguatezza o di garanzie appropriate, sono eccezionalmente ammessi Trasferimenti successivi solo se si applica una deroga ai sensi dell'articolo 49 del GDPR (es. in caso di trasferimento necessario per importanti motivi di interesse pubblico).

#### 4.1.7. Accountability (Responsabilizzazione)

Ogni Società del gruppo American Express vincolata alle BCR che agisce in qualità di Titolare del trattamento è competente per il rispetto delle presenti BCR ed è in grado di comprovarlo. La conformità a tali requisiti comprende:

- la necessità di tenere registri elettronici delle attività di Trattamento svolte sui Dati personali trasferiti ai sensi delle presenti BCR, e a disposizione delle Autorità di controllo competenti su richiesta. Tali registri contengono le informazioni richieste dal GDPR, quali: il nome e i dati di contatto del Titolare del trattamento, del suo rappresentante e del DPO (ove applicabile), le finalità del Trattamento, le categorie di Interessati e le categorie di Dati personali, i destinatari dei Dati personali, i Trasferimenti verso Paesi al di fuori dello SEE unitamente alla documentazione delle garanzie adeguate implementate per legittimare tali Trasferimenti, i termini ultimi previsti per la cancellazione delle diverse categorie di Dati personali (ove possibile) e la descrizione delle misure di sicurezza applicate (ove possibile).

Ogni Società del gruppo American Express vincolata alle BCR che agisce come Responsabile del trattamento per conto di un'altra Società del gruppo American Express vincolata alle BCR terrà anche un registro elettronico delle attività di Trattamento svolte sui Dati Personalni trasferiti ai sensi delle presenti BCR per conto del rispettivo Titolare del trattamento. Tali registri devono includere le seguenti informazioni: il nome e i dati di contatto del Responsabile del trattamento e del rispettivo Titolare del trattamento e, ove applicabile, del rappresentante e del DPO sia del Responsabile del trattamento sia del Titolare del trattamento, le categorie di Trattamento gestite per conto del Titolare del trattamento, i Trasferimenti verso paesi al di fuori dello SEE unitamente alla documentazione delle garanzie adeguate implementate per legittimare tali Trasferimenti e alla descrizione delle misure di sicurezza applicate (ove possibile);

- lo svolgimento di Valutazioni d'impatto sulla protezione dei dati (applicabile solo qualora le attività di Trattamento presentino un potenziale rischio elevato per i diritti e le libertà degli Interessati); e
- qualora la Valutazione d'impatto sulla protezione dei dati (DPIA) indichi che le attività di Trattamento presenterebbero un rischio elevato, in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio, la Società del gruppo American Express vincolata alle BCR di riferimento che agisce in qualità di Titolare del trattamento deve, prima di procedere al Trattamento, consultare l'Autorità di controllo competente.

Inoltre, le Società del gruppo American Express vincolate alle BCR hanno adottato misure amministrative, tecniche e organizzative appropriate volte a implementare i principi di protezione dei dati, a facilitare la conformità ai requisiti stabiliti nelle presenti BCR (protezione dei dati fin dalla progettazione e di default) e a garantire che le attività di trattamento svolte dalle Società del gruppo American Express vincolate alle BCR siano adeguatamente documentate (anche nell'ambito del processo di approvazione dei nuovi prodotti e nel programma di Lifecycle Management delle terze parti).

#### 4.2. Diritti degli Interessati

- Diritti di essere informato, accesso, limitazione, opposizione, rettifica, cancellazione, diritto di revocare il consenso e alla portabilità dei dati

Le Società del gruppo American Express vincolate alle BCR soddisfano le richieste degli Interessati di esercitare i diritti previsti dal GDPR, ove applicabile. Più specificamente, American Express garantisce che l'Interessato possa esercitare i diritti riportati di seguito:

- essere informato (le informazioni sono contenute nell'Informativa sulla privacy di American Express che si applica alle attività di Trattamento svolte da American Express nell'ambito del rapporto che intercorre tra la società e l'Interessato);
- accesso ai propri Dati personali (diritto di accesso). L'Interessato ha il diritto di ricevere una copia dei Dati personali in nostro possesso e di verificarne la legittimità di Trattamento;
- limitazione del Trattamento dei Dati personali (diritto di limitazione del Trattamento). L'Interessato ha il diritto di richiedere la limitazione del Trattamento dei propri Dati personali quando ricorre una delle seguenti ipotesi:
  - l'Interessato richiede di verificare l'esattezza dei Dati personali;
  - il Trattamento è illecito e l'Interessato si oppone alla cancellazione dei propri Dati personali;

- benché American Express non ne abbia più bisogno ai fini del Trattamento, i Dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; oppure
- l'Interessato si è opposto al Trattamento dei propri Dati personali, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi di American Express rispetto a quelli dell'Interessato;

- opposizione al Trattamento dei Dati personali (diritto di opposizione), per i seguenti motivi:

- motivi connessi alla situazione particolare dell'Interessato, quando il fondamento giuridico applicabile è il legittimo interesse. In alcuni casi, potremmo dimostrare l'esistenza di motivi legittimi cogenti per procedere al Trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato. In tal caso, ne daremo comunicazione all'Interessato; e
- in caso di Trattamento per finalità di marketing diretto;

- rettifica dei Dati personali (diritto di rettifica). L'Interessato ha il diritto di ottenere la rettifica dei Dati personali incompleti o inesatti che lo riguardano; potrebbe essere necessaria, da parte di American Express, una verifica dell'esattezza dei nuovi dati forniti dall'Interessato;

- cancellazione dei Dati personali (diritto alla cancellazione o diritto all'oblio). L'Interessato ha il diritto di ottenere la cancellazione o l'eliminazione dei propri Dati personali qualora non sussistano validi motivi per proseguire il Trattamento. L'Interessato ha inoltre il diritto di ottenere la cancellazione o l'eliminazione dei propri Dati personali qualora abbia esercitato il proprio diritto di opposizione al Trattamento (si veda di seguito), qualora tali dati siano stati trattati illecitamente o qualora debbano essere cancellati per adempiere un obbligo legale (es. legge locale della Società del gruppo American Express vincolata alle BCR di riferimento situata al di fuori dello SEE). Tuttavia, American Express potrebbe non essere in grado di soddisfare in ogni momento la richiesta dell'Interessato per motivi specifici stabiliti dalla legge, che saranno notificati all'Interessato, se del caso, al momento della richiesta;

- revoca del consenso al Trattamento prestato in precedenza. Tale revoca non pregiudica la liceità del Trattamento basata sul consenso prima della revoca. In caso di revoca del consenso, American Express potrebbe non essere in grado di fornire all'Interessato determinati prodotti o servizi. Tale eventualità verrà comunicata al momento della revoca; e

- ricezione dei propri Dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico e/o trasmissione di tali dati a un

altro Titolare del trattamento (diritto alla portabilità dei dati). American Express trasmetterà all'Interessato, o (laddove tecnicamente possibile) a una terza parte scelta dallo stesso, i Dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico. Tale diritto si applica solo alle informazioni automatizzate per le quali l'Interessato ha inizialmente prestato il proprio consenso o qualora tali informazioni siano state utilizzate per l'esecuzione di un contratto con l'Interessato.

Inoltre, American Express comunicherà ai destinatari cui sono stati trasmessi i Dati personali dell'Interessato (salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato) l'eventuale esercizio del diritto di rettifica o cancellazione o limitazione del Trattamento dei Dati personali dell'Interessato. Su richiesta dell'Interessato, American Express comunicherà a quest'ultimo l'elenco di tali destinatari.

Le Società del gruppo American Express vincolate alle BCR sono soggette a specifiche policy inerenti alla gestione di tali richieste per garantire che l'Interessato abbia i mezzi per esercitare tali diritti. Se l'Interessato intende esercitare uno dei suoi diritti può contattare il DPO American Express all'indirizzo DPO-Europe@aexp.com.

- Processo decisionale automatizzato

Le Società del gruppo American Express vincolate alle BCR assicurano che l'Interessato non sia sottoposto a decisioni basate unicamente sul Trattamento automatizzato dei Dati personali, compresa la Profilazione, che producono effetti giuridici o effetti significativi analoghi, salvo se il Trattamento sia:

- necessario per la conclusione o l'esecuzione di un contratto tra l'Interessato e American Express;
- autorizzato da una legge a cui American Express è soggetta e che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'Interessato; oppure
- basato sul consenso esplicito dell'Interessato a tale Trattamento.

Qualora il Trattamento si basi sul Consenso dell'Interessato o sia necessario per la conclusione o l'esecuzione di un contratto tra l'Interessato e American Express, quest'ultima attuerà misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'Interessato, che prevedano almeno il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione.

In conformità a tali restrizioni, American Express ha la facoltà di utilizzare Trattamenti automatizzati che contribuiscono al processo decisionale della società, ad esempio per

individuare e gestire eventuali frodi (es. per valutare se il conto dell'Interessato viene utilizzato per scopi fraudolenti o per attività di riciclaggio o per stabilire se il conto è stato violato da truffatori) o per evadere le richieste relative alle Carte e valutarne i rischi di credito e sicurezza. Tali metodi vengono regolarmente testati per garantire che rimangano corretti, efficaci e imparziali.

L'Interessato può contattare il DPO American Express all'indirizzo DPO-Europe@aexp.com per esercitare il diritto di richiedere una verifica manuale di alcune attività di Trattamento automatizzate che possono avere un impatto sui diritti legali o altri diritti contrattuali dell'Interessato o che possono avere un effetto giuridico analogo.

## 5. RETE DPO DI AMERICAN EXPRESS

American Express ha nominato un DPO, incaricato di monitorare la conformità alle BCR, a cui viene garantito il massimo supporto da parte del management per l'adempimento di tale compito. Il DPO, nominato in base alle sue qualità professionali, riporta al Chief Privacy Officer di American Express e ha accesso al Consiglio di Amministrazione di American Express Company attraverso il sistema di reporting diretta del Chief Privacy Officer.

Di seguito vengono riportate le attività di competenza del DPO:

- informare e fornire consulenza alle società del gruppo American Express e ai Dipendenti American Express in merito ai loro obblighi ai sensi della Normativa applicabile in materia di protezione dei dati;
- monitorare la conformità alla Normativa applicabile in materia di protezione dei dati (comprese la formazione e la conformità a livello locale) attraverso la valutazione degli indicatori di rischio e dei controlli chiave. Il DPO riferisce i risultati di tali attività di monitoraggio al forum di governance interno di livello senior competente;
- fornire consulenza in merito alle Valutazioni d'impatto sulla protezione dei dati e monitorarne l'esecuzione;
- riferire su questioni, rischi e risultati in materia di privacy al Consiglio di amministrazione di AEESA e ai comitati di rischio subordinati, a seconda dei casi;
- fornire consulenza in merito alle nuove leggi e regolamenti in materia di privacy e all'impatto dei processi esistenti;

- fornire consulenza sulla conformità alle presenti BCR;
- collaborare con le Autorità di controllo; e
- fungere da punto di contatto per le Autorità di controllo (anche, ad esempio, in caso di violazione dei dati personali da denunciare alle autorità).

La nomina viene comunicata alle Autorità di controllo dei Paesi europei in cui American Express è presente.

Il DPO lavora a stretto contatto ed è supportato da una rete di specialisti della privacy e di avvocati specializzati nella compliance dislocati in ogni mercato europeo che monitorano la conformità alle Normative applicabili in materia di protezione dei dati nella loro regione e segnalano al DPO le questioni più importanti in materia di privacy. Il DPO è supportato nello svolgimento delle attività di sua competenza dal Global Privacy Office sotto la guida del Chief Privacy Officer di American Express. Di seguito viene riportata una sintesi del ruolo e delle attività della rete per la privacy:

- Il Global Privacy Office ("GPO") riporta al Chief Privacy Officer di American Express. Le responsabilità del GPO comprendono le funzioni di supervisione del rischio di privacy a livello globale in tutta l'organizzazione e la gestione del framework generale del Privacy Program di American Express.
- I Compliance Privacy Subject Matter Expert (individualmente o in gruppo) fungono da esperti locali della conformità in materia di privacy per le persone giuridiche locali.
- Gli avvocati specializzati in privacy di American Express forniscono interpretazioni in materia di Protezione dei dati e indicazioni sui requisiti di legge alle persone potenzialmente interessate da rischi di privacy.
- La prima linea del Privacy Practice Centre of Excellence è responsabile di fornire supporto alle business unit per l'implementazione di controlli, policy, standard e requisiti in materia di privacy.
- L'Information Security Office è responsabile di informare il DPO e il GPO UE in merito a eventuali rischi per la sicurezza informatica e delle informazioni.

Il DPO è supportato nello svolgimento delle attività di sua competenza dal Global Privacy Office sotto la guida del Chief Privacy Officer di American Express. È possibile contattare direttamente il DPO mediante i dati di contatto indicati nella sezione 9.

## 6. FORMAZIONE E CONSAPEVOLEZZA

Tutte le Società del gruppo American Express vincolate alle BCR mettono a disposizione materiale e corsi di formazione adeguati e aggiornati per tutti i Dipendenti, in particolare per i Dipendenti che si occupano di raccogliere e trattare Dati personali, che hanno accesso permanente o abituale a tali dati o che sono coinvolti nello sviluppo di strumenti utilizzati per il Trattamento dei Dati personali, affinché siano consapevoli dei loro obblighi ai sensi della Normativa applicabile in materia di protezione dei dati e delle presenti BCR (tale formazione riguarda, tra gli altri aspetti, le procedure di gestione delle richieste di accesso ai Dati personali da parte delle autorità pubbliche).

Si tratta di corsi obbligatori per i quali viene monitorato il completamento. La frequenza di partecipazione a tali corsi varia a seconda del ruolo, della funzione e delle attività che prevedono l'accesso ai Dati personali del Dipendente.

American Express organizza inoltre un corso annuale obbligatorio in materia di Protezione dei dati rivolto a tutti i Dipendenti, per il quale viene monitorato il completamento.

## 7. AUDIT E CONTROLLI

American Express ha implementato un programma di conformità che prevede regolari audit e controlli di conformità delle operazioni delle Società del gruppo American Express vincolate alle BCR (svolti da auditor interni o, se necessario, esterni) per assicurare che le BCR e tutte le relative policy e procedure siano rispettate e aggiornate e, in caso di segnalazioni di non conformità, per controllare e verificare il rispetto delle BCR.

Gli audit sulla Protezione dei dati coprono tutti gli aspetti delle BCR (es. applicazioni, sistemi IT, trasferimenti successivi, ecc.), compresi i metodi per garantire che le misure correttive e gli action plan verranno adottati e (se necessario) siano stati implementati.

La frequenza degli audit viene determinata sulla base dei rischi che le attività di Trattamento coperte dalle presenti BCR comportano per i diritti e le libertà degli Interessati. Vengono effettuati audit regolari con cadenza biennale con un approccio basato sul rischio.

Ulteriori audit sulla protezione dei dati possono essere richiesti dal DPO di propria iniziativa, su richiesta della rete di specialisti della privacy di American Express o su specifica richiesta di una delle Società del gruppo American Express vincolate alle BCR. Il gruppo di audit interno di American Express, in quanto organo di controllo indipendente, valuterà l'opportunità e la fattibilità di queste richieste di audit in base al proprio quadro di valutazione del rischio.

La pianificazione e il programma degli audit e l'entità responsabile dell'esecuzione degli audit di conformità alle BCR saranno determinati dal dipartimento di American Express che richiede tale audit. L'indipendenza dei dipartimenti competenti (e di coloro che sono incaricati di svolgere l'audit) è garantita in relazione a qualsiasi richiesta di audit e allo svolgimento delle attività di propria competenza relative a tale audit.

In caso di audit effettuati da auditor esterni, si applicano le seguenti condizioni per l'affidamento dell'incarico:

- l'auditor esterno deve essere indipendente e in possesso delle opportune qualifiche, deve aver ottenuto un'autorizzazione di sicurezza appropriata e non deve essere un concorrente di American Express o dei fornitori della società.
- l'ambito di applicazione, i termini e la durata dell'audit saranno concordati con l'auditor esterno prima dello svolgimento dell'audit.
- l'auditor esterno sarà soggetto ad appropriati obblighi di riservatezza ai sensi di un contratto in forma scritta stipulato tra l'auditor e American Express.

I risultati di questi audit e controlli di conformità saranno comunicati al Global Privacy Office di American Express, al DPO, al Consiglio di amministrazione di AEESA, alle Autorità di controllo competenti (se richiesto da un'Autorità di controllo competente) e, se del caso, saranno messi a disposizione del Comitato Audit del Consiglio di amministrazione di American Express Company.

Qualora venga riscontrato una lacuna di conformità, la Società del gruppo American Express vincolata alle BCR di riferimento dovrà seguire qualsiasi linea guida specifica ricevuta dal DPO per garantire la verifica della conformità alle BCR. Qualora la Società del gruppo American Express vincolata alle BCR di riferimento non possa adeguarsi a tali linee guida specifiche a causa di leggi o prassi locali, ci si dovrà attenere alla procedura descritta nella sezione 11.1 delle presenti BCR.

American Express collaborerà inoltre con eventuali controlli di conformità condotti da qualsiasi Autorità di controllo con il foro competente, indipendentemente dal fatto che siano avviati in risposta a un reclamo da parte di un Interessato o su iniziativa dell'Autorità di controllo stessa.

## 8. CONFORMITÀ, ESECUZIONE E RESPONSABILITÀ

### 8.1. Responsabilità delle Società del gruppo American Express vincolate alle BCR

Ogni Società del gruppo American Express vincolata alle BCR è responsabile della conformità alle presenti BCR. Oltre alle responsabilità individuali delle Società del gruppo American Express vincolate alle BCR, AEESA si assumerà la responsabilità per qualsiasi violazione delle BCR compiuta da una Società del gruppo American Express

vincolata alle BCR situata in un Paese terzo. AEESA avrà la facoltà e accetta di intraprendere qualsiasi azione necessaria per porre rimedio agli atti o alle omissioni compiute da una Società del gruppo American Express vincolata alle BCR che tratta Dati personali in violazione delle BCR.

AEESA è tenuta a pagare il risarcimento dovuto per qualsiasi danno materiale o non materiale subito da un Interessato derivante da qualsiasi violazione delle BCR da parte di una Società del gruppo American Express vincolata alle BCR situata in un Paese terzo. Ogni risarcimento erogato sarà volto alla piena soddisfazione della richiesta di risarcimento dell'Interessato nei confronti delle Società del gruppo American Express vincolate alle BCR. Al fine di evitare equivoci, la responsabilità di AEESA si estende agli atti o alle omissioni di qualsiasi Società del gruppo American Express vincolate alle BCR situata in un Paese terzo che viola le BCR.

Se una Società del gruppo American Express vincolate alle BCR (anche nel caso in cui tale società sia situata in un Paese terzo) viola le BCR, i tribunali europei competenti avranno giurisdizione in merito a tale violazione. Qualora una Società del gruppo American Express vincolata alle BCR situata in un Paese terzo violi le BCR, gli Interessati, le Autorità di controllo e i tribunali competenti possono esercitare i propri diritti e presentare un reclamo contro AEESA come se tale comportamento fosse stato messo in atto da AEESA nello Stato Membro in cui ha sede (per ulteriori informazioni su come proporre reclamo, fare riferimento alla sezione 9 di seguito). Qualora una Società del gruppo American Express vincolata alle BCR situata nello SEE violi le norme BCR, gli Interessati possono esercitare i propri diritti ai sensi delle presenti BCR nei confronti di tale Società del gruppo American Express vincolata alle BCR (per ulteriori informazioni su come proporre reclamo, fare riferimento alla sezione 9 di seguito).

## 8.2. Diritti del terzo beneficiario

Ogni Interessato ha la facoltà di far valere, nei confronti di AEESA o di qualsiasi Società del gruppo American Express vincolata alle norme BCR, i termini delle seguenti disposizioni delle BCR in qualità di terzo beneficiario:

- principi di protezione dei dati (sezioni da 4.1.1 a 4.1.6 inclusa);
- facile accesso alle BCR (sezione 1.2);
- diritti degli Interessati (sezione 4.2);
- giurisdizione e responsabilità (sezione 8.1);
- la presente clausola relativa ai diritti del terzo beneficiario (sezione 8.2);

- diritto di proporre reclamo attraverso il meccanismo di reclamo interno di American Express (sezione 9);
- diritto a ricorsi giurisdizionali, diritto di ricorso effettivo e, se del caso, diritto di risarcimento in caso di violazione di uno degli elementi aventi efficacia esecutiva delle BCR, come stabilito nella presente sezione 8.2, nonché il diritto di proporre reclamo all'Autorità di controllo e al tribunale europeo competente (ricorsi giurisdizionali, ricorsi effettivi e risarcimento) (sezione 9);
- collaborazione con le Autorità di controllo (sezione 10);
- diritto internazionale privato relativamente alla conformità alle BCR e alle richieste di accesso governativo (sezione 11); e
- dovere di informare gli Interessati in merito a eventuali aggiornamenti delle BCR e dell'elenco dei membri BCR-C (sezione 14).

Tali diritti non si estendono agli elementi delle BCR relativi ai meccanismi interni implementati nelle Società del gruppo American Express vincolate alle BCR, come ad esempio dettagli inerenti la formazione, programma dell'audit, rete di compliance e relative modalità di aggiornamento.

### 8.3. Onere della prova

Qualora l'Interessato sia in grado di dimostrare di aver subito un danno e fornisca prove a dimostrazione della probabilità che tale danno si sia verificato a causa di una violazione delle BCR, ad AEESA spetta l'onere della prova a dimostrazione che la Società del gruppo American Express vincolata alle BCR situata in un Paese terzo non è responsabile di alcuna presunta violazione delle BCR, da cui possa derivare la richiesta di risarcimento danni da parte dell'Interessato o che tale violazione non ha avuto luogo.

Qualora AEESA sia in grado di dimostrare che una Società del gruppo American Express vincolata alle BCR situata in un Paese terzo non è responsabile dell'evento da cui è dipeso il danno, AEESA e la società in questione possono esonerarsi da tale responsabilità.

## 9. COME PROPORRE RECLAMO E FAR RISPETTARE LE BCR UE?

Qualora l'Interessato desideri presentare un reclamo o una richiesta di risarcimento ed esercitare i propri diritti nell'ambito delle presenti BCR (anche in relazione a qualsiasi Società del gruppo American Express vincolata alle BCR), può contattare in qualsiasi momento il DPO come segue: (a) per iscritto rivolgendosi alla sede di AEESA presso American Express Europe SA, Avenida Partenón 12 - 14, 28042 Madrid / SPAGNA;

oppure (b) tramite e-mail all'indirizzo [DPO-Europe@aexp.com](mailto:DPO-Europe@aexp.com). American Express incoraggia gli Interessati a utilizzare una delle modalità di contatto sopra elencate, ma non sussiste alcun obbligo in merito.

Il nostro team dedicato alla gestione dei reclami si occuperà delle segnalazioni ricevute per iscritto dagli Interessati senza ingiustificato ritardo e, comunque, al più tardi entro un mese. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste; in tal caso American Express informerà l'Interessato di tale proroga per iscritto.

Si noti che:

- Se il reclamo viene accolto, la Società del gruppo American Express vincolata alle BCR di riferimento adotterà le misure correttive appropriate per risolvere il reclamo e garantire la conformità alle BCR, a seconda dei casi;
- Se il reclamo viene respinto, American Express spiegherà all'Interessato le ragioni di tale decisione / la questione sarà riferita al DPO che riesaminerà il caso e comunicherà al reclamante la sua scelta di accettare la decisione originale oppure di procedere a una nuova decisione entro un (1) mese di calendario; e
- Se il reclamo subisce un ingiustificato ritardo, l'Interessato deve avvisare il DPO che, senza ingiustificato ritardo e comunque entro dieci (10) giorni lavorativi, chiarirà le ragioni di tale ritardo e renderà note le azioni intraprese fino a quel momento.

In aggiunta alla procedura di reclamo sopra descritta, gli Interessati possono presentare ricorso effettivo attraverso le seguenti modalità (anche in caso di reclami risolti senza la piena soddisfazione dell'Interessato). Si specifica che i diritti riportati di seguito possono essere esercitati indipendentemente dalla scelta dell'Interessato di seguire la procedura di reclamo riportata in precedenza:

- proporre reclamo all'Autorità di controllo nello Stato membro in cui l'Interessato risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione;
- ricorrere alle autorità giurisdizionali competenti dello Stato membro in cui ha sede la Società del gruppo American Express vincolata alle BCR di riferimento o in cui l'Interessato risiede abitualmente e, se del caso, ottenere il risarcimento dei danni subiti dall'Interessato come conseguenza di una violazione dei summenzionati Diritti del terzo beneficiario.

Tutte le Società del gruppo American Express vincolate alle BCR 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(1) del GDPR.

## 10. OBBLIGO DI COLLABORAZIONE CON LE AUTORITÀ DI CONTROLLO

Tutte le Società del gruppo American Express vincolate alle BCR sono tenute a:

- collaborare con qualsiasi Autorità di controllo competente e accettare di essere soggette a controlli e audit dalle stesse (incluso, se necessario, *in loco*) per qualsiasi questione riguardante le presenti BCR;
- tener conto del parere di tali Autorità di controllo per qualsiasi questione riguardante le presenti BCR; e
- attenersi alle decisioni di qualsiasi Autorità di controllo competente, fatto salvo il diritto di contestare o presentare ricorso nei confronti di tali conclusioni o decisioni, per qualsiasi questione riguardante le presenti BCR.

Tutte le Società del gruppo American Express vincolate alle BCR saranno tenute a fornire alle Autorità di controllo competenti, su richiesta, qualsiasi informazione in merito alle attività di Trattamento coperte dalle presenti BCR.

Qualsiasi controversia relativa all'esercizio dei poteri di supervisione dell'Autorità di controllo competente in merito alla conformità alle BCR sarà risolta dai tribunali dello Stato membro di tale Autorità di controllo, in conformità al diritto processuale di tale Stato membro. Le Società del gruppo American Express vincolate alle BCR di riferimento sono soggette alla giurisdizione di tali tribunali.

## 11. COME GESTIARE POTENZIALI CONFLITTI NORMATIVI E AFFRONTARE LE RICHIESTE DI ACCESSO DA PARTE DELLE AUTORITÀ GOVERNATIVE?

### 11.1. Leggi e prassi locali che impattano la conformità alle BCR UE

Ciascuna Società del gruppo American Express vincolata alle BCR utilizzerà le BCR come strumento per i Trasferimenti esclusivamente dopo aver accertato che le leggi e le prassi del Paese terzo applicabili al Trattamento dei Dati personali da parte della Società del gruppo American Express vincolata alle BCR di riferimento, che agisce in qualità di Importatore di dati (compresi eventuali obblighi di divulgazione dei Dati personali o misure che autorizzino l'accesso da parte di autorità pubbliche), non le impediscano di adempiere agli obblighi derivanti dalle presenti BCR. Tali indicazioni si basano sul

presupposto che le leggi e le prassi che rispettano l'essenza dei diritti e delle libertà fondamentali, e si attengono alle misure necessarie e proporzionate in una società democratica, non sono in contraddizione con le presenti BCR laddove salvaguardano uno dei seguenti obiettivi (come riportati nell'Articolo 23, paragrafo 1, del GDPR):

- (a) la sicurezza nazionale;
- (b) la difesa;
- (c) la sicurezza pubblica;
- (d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
- (e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
- (f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
- (g) le attività volte a prevenire, indagare, accettare e perseguire violazioni della deontologia delle professioni regolamentate;
- (h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
- (i) la tutela dell'interessato o dei diritti e delle libertà altrui;
- (j) l'esecuzione delle azioni civili.

Nell'analisi delle leggi e delle prassi del Paese terzo che possono avere un impatto sulla conformità alle disposizioni delle BCR, le Società del gruppo American Express vincolate alle BCR hanno tenuto (e terranno) in debita considerazione, in particolare, i seguenti elementi:

i. Le circostanze specifiche del Trasferimento o del complesso di Trasferimenti e di qualsiasi Trasferimento successivo previsto all'interno dello stesso Paese terzo o verso un altro Paese terzo, tra cui:

- le finalità del trasferimento e del trattamento dei dati (es. HR, conservazione, supporto informatico);
- i tipi di soggetti coinvolti nel Trattamento (l'Importatore di dati e qualsiasi altro destinatario di eventuali Trasferimenti successivi);
- il settore economico in cui 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. Le leggi e le prassi del Paese terzo che risultano rilevanti in base alle circostanze dei Trasferimenti, comprese quelle che prevedono la divulgazione dei Dati personali alle autorità pubbliche o che autorizzano l'accesso da parte di tali autorità, e quelle che prevedono l'accesso a tali dati durante il transito tra il Paese dell'Esportatore di dati e quello dell'Importatore di dati, nonché le limitazioni e le garanzie applicabili.
- iii. Eventuali garanzie contrattuali, organizzative o tecniche adottate per integrare le garanzie previste dalle BCR, comprese le misure applicate durante la trasmissione e al Trattamento dei dati personali nel Paese terzo di destinazione.

Nel caso in cui debbano essere implementate garanzie aggiuntive rispetto a quelle previste dalle BCR, AEESA, il DPO e la rete di specialisti della privacy di American Express ne riceveranno relativa comunicazione e saranno coinvolti in tale valutazione.

L'Esportatore di dati dovrà documentare in modo appropriato tale valutazione, nonché le misure supplementari selezionate e implementate. L'Esportatore di dati fornirà la documentazione alle Autorità di controllo competenti su richiesta.

Qualora un Importatore di dati abbia motivo di ritener che, nell'ambito della sua adesione alle presenti BCR e in fase di applicazione delle stesse come strumento per i Trasferimenti, sia o sia diventato soggetto a leggi o prassi che gli impedirebbero di adempiere agli obblighi derivanti dalle BCR (anche a seguito di una modifica delle leggi del Paese terzo o di un provvedimento (come una richiesta di divulgazione)), l'Importatore di dati dovrà tempestivamente comunicarlo all'Esportatore di dati e informerà AEESA. Verrà inoltre seguita la procedura indicata di seguito:

- L'Importatore di dati comunicherà tempestivamente quanto sopra all'Esportatore di dati e informerà AEESA.
- A seguito della verifica di tale segnalazione, l'Esportatore di dati, insieme ad AEESA, al DPO e alla rete di specialisti della privacy di American Express, individuerà tempestivamente le misure supplementari (es. misure organizzative o tecniche per garantire la sicurezza e la riservatezza) che l'Esportatore di dati e/o il rispettivo Importatore di dati dovranno adottare, al fine di consentire loro di adempiere agli obblighi derivanti dalle BCR. Questa procedura si applica anche qualora l'Esportatore di dati abbia motivo di ritener che il rispettivo Importatore di dati non sia più in grado di adempiere agli obblighi derivanti dalle BCR.
- Qualora l'Esportatore di dati, insieme ad AEESA, al DPO e alla rete di specialisti della privacy di American Express, ritenga che non sia possibile rispettare le BCR - anche se integrate da misure supplementari - per un Trasferimento o un complesso di Trasferimenti, o qualora riceva tale indicazione dall'Autorità di

controllo competente (o dalle Autorità), l'Esportatore di dati sospenderà il Trasferimento o il complesso di Trasferimenti in questione, nonché tutti i Trasferimenti per i quali la stessa valutazione e lo stesso ragionamento porterebbero a un risultato analogo, fino al momento in cui la conformità sarà nuovamente garantita o il Trasferimento sarà terminato.

- A seguito di tale sospensione, l'Esportatore di dati porrà fine al Trasferimento o al complesso di Trasferimenti qualora le BCR non possano essere rispettate e non sia possibile ripristinare la conformità alle BCR entro un mese dalla sospensione. In tal caso, i Dati personali trasferiti prima della sospensione e le loro eventuali copie dovranno essere restituiti o distrutti nella loro totalità, a discrezione dell'Esportatore di dati.
- AEESA, il DPO e la rete di specialisti della privacy di American Express informeranno tutte le altre Società del gruppo American Express vincolate alle BCR della valutazione effettuata e dei relativi risultati, affinché le misure supplementari identificate siano applicate nel caso in cui lo stesso tipo di Trasferimenti sia effettuato da qualsiasi altra Società del gruppo American Express vincolata alle BCR o, laddove non sia stato possibile adottare misure supplementari efficaci, i Trasferimenti in questione siano sospesi o interrotti.

Ciascun Esportatore di dati monitorerà, su base continuativa e, se del caso, in collaborazione con i propri Importatori di dati, gli eventuali sviluppi nei Paesi terzi verso i quali gli Esportatori di dati hanno trasferito Dati personali che potrebbero avere un impatto sulla valutazione iniziale del livello di protezione e sulle decisioni prese di conseguenza in merito a tali Trasferimenti.

## 11.2 Obblighi dell'Importatore di dati in caso di richieste di accesso governativo

In aggiunta all'obbligo dell'Importatore di dati di informare il rispettivo Esportatore di dati dell'impossibilità di adempiere alle disposizioni delle presenti BCR, e fatto salvo tale obbligo (come indicato nella sezione 11.1 di cui sopra), l'Importatore di dati invierà una notifica tempestiva all'Esportatore di dati e, ove possibile, all'Interessato (se necessario, con la collaborazione dell'Esportatore di dati) qualora:

- a) riceva una richiesta giuridicamente vincolante da parte di un'autorità pubblica ai sensi delle leggi del Paese terzo, o di un altro Paese terzo, in merito alla divulgazione dei Dati personali trasferiti ai sensi delle presenti BCR. Tale notifica includerà informazioni sui Dati personali richiesti, sull'autorità richiedente, sul fondamento giuridico della richiesta e sulla risposta fornita; e/o
- b) venga a conoscenza di eventuali accessi diretti da parte di autorità pubbliche ai Dati personali trasferiti ai sensi delle presenti BCR in conformità alle leggi del paese di destinazione. In questo caso, tale notifica includerà tutte le informazioni in possesso dell'Importatore di dati.

In caso di divieto di notifica all'Esportatore di dati e/o all'Interessato coinvolto (o agli Interessati coinvolti), l'Importatore di dati compirà ogni ragionevole sforzo per ottenere una deroga a tale divieto, al fine di comunicare il maggior numero di informazioni possibile e nel più breve tempo possibile. L'Importatore di dati documenterà i propri sforzi per poterne fornire dimostrazione su richiesta dell'Esportatore di dati.

L'Importatore di dati fornirà all'Esportatore di dati, a intervalli regolari, il maggior numero possibile di informazioni utili in merito alle richieste ricevute (in particolare, numero di richieste, tipologia di dati richiesti, autorità richiedente/i, eventuali ricorsi presentati a fronte di una richiesta con il relativo esito, ecc.). Qualora venga imposto divieto, anche solo parziale, all'Importatore di dati relativamente alla comunicazione delle informazioni - di cui sopra - all'Esportatore di dati, ne informerà l'Esportatore di dati senza ingiustificato ritardo.

L'Importatore di dati conserverà le informazioni - di cui sopra - per tutto il tempo in cui i Dati personali saranno soggetti alle garanzie previste dalle BCR e le fornirà alle Autorità di controllo competenti su richiesta.

L'Importatore di dati esaminerà la legittimità della richiesta di divulgazione, verificando in particolare che rientri nei poteri concessi all'autorità pubblica richiedente, e presenterà ricorso qualora, dopo un'attenta valutazione, emergeranno ragionevoli motivi per ritenere che la richiesta sia illegittima ai sensi delle leggi del paese di destinazione, degli obblighi applicabili ai sensi del diritto internazionale e dei principi della cortesia internazionale. In tali circostanze:

- L'Importatore di dati, alle medesime condizioni, presenterà ricorso.
- In caso di ricorso, l'Importatore di dati chiederà misure provvisorie al fine di sospendere gli effetti della richiesta fino alla decisione finale dell'autorità giudiziaria competente. I Dati personali richiesti non saranno divulgati fino al momento in cui sarà emesso obbligo di procedere in tal senso in base alle norme procedurali applicabili.

L'Importatore di dati documenterà la propria valutazione giuridica e l'eventuale ricorso presentato nei confronti della richiesta di divulgazione e, nella misura consentita dalle leggi del paese di destinazione, metterà la documentazione a disposizione dell'Esportatore di dati e, su richiesta, a disposizione delle Autorità di controllo competenti.

L'Importatore di dati fornirà la quantità minima consentita di informazioni in risposta a una richiesta di divulgazione, sulla base di una ragionevole interpretazione della richiesta stessa.

In ogni caso, i Trasferimenti di Dati personali da parte di una Società del gruppo American Express vincolata alle BCR a qualsiasi autorità pubblica non saranno massivi, sproporzionali e indiscriminati e si limiteranno a quanto necessario in una società

democratica. Tale limitazione si applica a qualsiasi richiesta legalmente vincolante di divulgazione di Dati personali da parte di un'autorità preposta all'applicazione della legge o di un organismo preposto alla sicurezza nazionale.

### 11.3. Correlazione tra leggi nazionali e BCR UE

Qualora la Normativa applicabile in materia di protezione dei dati richieda un livello di protezione più elevato per i Dati personali, tali leggi sulla protezione dei dati prevarranno sulle presenti norme BCR.

## 12. NON CONFORMITÀ ALLE BCR UE

Tutte le Società del gruppo American Express vincolate alle BCR accettano quanto segue:

- Saranno effettuati Trasferimenti verso un'altra Società del gruppo American Express vincolata alle BCR solo a condizione che tale Entità sia effettivamente vincolata dalle BCR e possa garantire la conformità alle stesse.
- L'Importatore di dati informerà tempestivamente l'Esportatore di dati qualora non sia in grado di rispettare le BCR, per qualsiasi motivo, comprese le situazioni descritte in dettaglio nella sezione 11, di cui sopra.
- Qualora l'Importatore di dati violi le BCR o non sia in grado di rispettarle, l'Esportatore di dati sosponderà il Trasferimento.
- L'Importatore di dati, a esclusiva discrezione del rispettivo Esportatore di dati, restituirà o cancellerà immediatamente i Dati personali, trasferiti ai sensi delle presenti BCR nella loro totalità, qualora:
  - l'Esportatore di dati abbia sospeso il Trasferimento e la conformità alle BCR non venga ripristinata entro un tempo ragionevole, e in ogni caso entro un mese dalla sospensione; oppure
  - sia in corso una violazione rilevante o ripetuta delle BCR da parte dell'Importatore di dati; oppure
  - l'Importatore di dati non si conformi a una decisione vincolante emessa da un tribunale competente o da un'Autorità di controllo competente in merito ai suoi obblighi derivanti dalle BCR.

Gli obblighi di cui sopra si applicheranno a qualsiasi copia dei Dati personali e l'Importatore di dati certificherà la cancellazione di tali dati all'Esportatore di dati.

Fino al momento in cui i dati vengono cancellati o restituiti, l'Importatore di dati continuerà a garantire la conformità alle BCR.

Se l'Importatore di dati è soggetto a leggi locali che vietano la restituzione o la cancellazione dei Dati personali trasferiti, l'Importatore di dati assicura che continuerà a garantire la conformità al e tratterà i Dati personali solo nella misura e per il tempo richiesti ai sensi di tale legge locale.

### 13. CESSAZIONE

Se un Importatore di Dati cessa di essere vincolato dalle BCR, la Società del gruppo American Express vincolata alle BCR può conservare, restituire o cancellare i Dati personali ricevuti ai sensi delle BCR, a condizione che, qualora l'Importatore di dati e il rispettivo Esportatore di dati concordino la facoltà per l'Importatore di dati di conservare i Dati personali, l'Importatore di dati garantisca la protezione di tali Dati personali in conformità ai requisiti di cui al Capitolo 5 (trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali) del GDPR, ovvero:

- L'Importatore di dati potrà trasferire tali Dati personali esclusivamente se è stata implementata una garanzia adeguata;
- L'Importatore di dati continuerà a rispettare le BCR in relazione a tali Dati personali, al fine di garantirne la protezione; e
- L'Importatore di dati tratterà i Dati personali solo nella misura e per il tempo necessari alla finalità per cui tali dati sono conservati dall'Importatore di dati.

### 14. AGGIORNAMENTI ALLE BCR UE

American Express ha la facoltà di aggiornare i termini delle presenti BCR per recepire, ad esempio, modifiche del contesto normativo o della struttura societaria. American Express si impegna a comunicare eventuali modifiche alle BCR senza ingiustificato ritardo a tutte le Società del gruppo American Express vincolate alle BCR.

Eventuali modifiche alle BCR o all'elenco delle Società del gruppo American Express vincolate alle BCR saranno comunicate con cadenza annuale alle Autorità di controllo competenti tramite l'Autorità di controllo capofila specificando brevemente le ragioni degli aggiornamenti. Le Autorità di controllo competenti riceveranno comunicazione anche nel caso in cui non siano state apportate modifiche.

Qualora una modifica possa avere un impatto sul livello di protezione offerto dalle presenti BCR o avere un impatto significativo sulle stesse (es. modifiche al carattere vincolante, modifiche della Società del gruppo American Express vincolata alle BCR responsabile di violazioni delle BCR, ecc.), sarà tempestivamente e preventivamente comunicata alle Autorità di controllo competenti tramite l'Autorità di controllo capofila,

specificando brevemente le ragioni degli aggiornamenti. In questo caso, l'Autorità di controllo valuterà anche se le modifiche apportate richiedono una nuova approvazione.

American Express ha identificato un team (la funzione Global Privacy Office) che gestisce un elenco costantemente aggiornato delle Società del gruppo American Express vincolate alle BCR, tiene traccia e registra tutti gli aggiornamenti normativi e fornisce le informazioni necessarie agli Interessati oppure, su richiesta, alle Autorità di controllo competenti. Inoltre, le Società del gruppo American Express vincolate alle BCR effettueranno Trasferimenti a una nuova Società del gruppo American Express vincolate alle norme BCR esclusivamente a partire dal momento in cui tale entità sarà effettivamente vincolata dalle presenti BCR e sarà in grado di garantire la conformità alle stesse.

#### APPENDICE 1 - NATURA E FINALITÀ DEI TRASFERIMENTI DI DATI PERSONALI NELL'AMBITO DELLE BCR

Tipologia di trattamento e finalità	Categorie di Dati personali
<b>Categorie di Interessati: Dipendenti</b>	
Per il Trattamento dei dati dei Dipendenti per emergenza medica	Indirizzo e-mail; ID dipendente/Customer Employment ID; nome della persona fisica (cognome + nome/iniziale); telefono/cellulare personale/fax
Per finalità fiscali, se previsto dalla legislazione dello Stato membro a cui il Titolare del trattamento di riferimento è soggetto	Informazioni sui figli (età/genere, informazioni di contatto, ecc.); disabilità / alloggio su base normativa; reddito; sentenze o procedimenti giudiziari; nazionalità; numero di conto (completo/parziale/criptato); domanda e/o risposte di sicurezza / verifica; numero di Green card/Alien resident card; Carta di Identità; numero di previdenza sociale (completo/parziale/criptato); informazioni sui figli (età/genere, informazioni di contatto, ecc.); sentenze o procedimenti giudiziari; iscrizione a sindacati o associazioni; nazionalità; ricezione di assegni di mantenimento per i figli, alimenti o mantenimento separato; ricezione di assistenza statale (es. sussidi statali); età; fascia retributiva; dati ROC relativi ai contributi di beneficenza; data di nascita; livello di istruzione; indirizzo e-mail; ID dipendente/Customer Employment ID; nome del datore di lavoro; storia o stato occupazionale; indicatore di famiglia con figli; nome della persona

Tipologia di trattamento e finalità	Categorie di Dati personali
	fisica (cognome + nome/iniziale); tipologia di congedo; stato civile o di famiglia; storico dei pagamenti; data di pensionamento; data di cessazione; indirizzo; codice fiscale; telefono/cellulare personale/fax
Per adempiere agli obblighi derivanti dal contratto di lavoro del dipendente, ad esempio per elaborare la busta paga, versare lo stipendio, gestire i benefit aziendali (compresi quelli medici, assicurativi e pensionistici) e adempiere agli obblighi di legge previsti dal contratto di lavoro.	Data di cessazione; data di pensionamento; informazioni sui figli (età/genere, informazioni di contatto, ecc.); disabilità / alloggio su base normativa; sentenze o procedimenti giudiziari; numero di conto (completo/parziale/criptato); domanda e/o risposte di sicurezza / verifica; numero di Green card/Alien resident card; informazioni sui figli (età/genere, informazioni di contatto, ecc.); sentenze o procedimenti giudiziari; iscrizione a sindacati o associazioni; ricezione di assegni di mantenimento per i figli, alimenti o mantenimento separato; ricezione di assistenza statale (es. sussidi statali); dati ROC relativi ai contributi di beneficenza; storia o stato occupazionale; indicatore di famiglia con figli; storico dei pagamenti; numero di conto (completo/parziale/criptato) - Altri istituti di pagamento; numero di patente di guida; Carta di Identità; numero di previdenza sociale (completo/parziale/criptato); reddito; nazionalità; età; fascia retributiva; data di nascita; livello di istruzione; indirizzo e-mail; ID dipendente/Customer Employment ID; nome del datore di lavoro; genere; origine etnica; nome della persona fisica (cognome + nome/iniziale); tipologia di congedo; stato civile o di famiglia; occupazione; data di pensionamento; data di cessazione; indirizzo; codice fiscale; telefono/cellulare personale/fax; username
Per gestire richieste di risarcimento e controversie legate al rapporto di lavoro con i dipendenti.	Numero di passaporto; nazionalità; fascia retributiva; data di nascita; indirizzo e-mail; ID dipendente/Customer Employment ID; storia o stato occupazionale; nome della persona fisica (cognome + nome/iniziale); fotografia; indirizzo; telefono/cellulare personale/fax; dati biometrici; informazioni sui figli (età/genere, informazioni di contatto, ecc.)

Tipologia di trattamento e finalità	Categorie di Dati personali
Per svolgere performance review e determinare i requisiti di prestazione.	Fascia retributiva; livello di istruzione; ID dipendente/Customer Employment ID; storia o stato occupazionale; genere; nome della persona fisica (cognome + nome/iniziale); valutazione delle prestazioni; occupazione; data di cessazione
Per tutelare, salvaguardare e monitorare la salute e la sicurezza dei dipendenti American Express.	Informazioni sanitarie protette (PHI); ID dipendente/Customer Employment ID; nome della persona fisica (cognome + nome/iniziale); indirizzo e-mail; fascia retributiva; nome del datore di lavoro
Per amministrare e gestire i benefit aziendali e qualsiasi altro incentivo o programma a cui i dipendenti partecipano, compresa la gestione e/o la richiesta di buoni pasto cartacei e/o elettronici.	Numero di passaporto; ID dipendente/Customer Employment ID; numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento; Informazioni sui figli (età/genere, informazioni di contatto, ecc.); informazioni sull'agente autorizzato/ sulla gestione del programma; stato cliente; nome del datore di lavoro; storico dei pagamenti; indirizzo; numero di conto (completo/parziale/criptato) - Altri istituti di pagamento; numero di patente di guida; Carta di Identità; numero di previdenza sociale (completo/parziale/criptato); disabilità / alloggio su base normativa; reddito; nazionalità; informazioni sanitarie protette (PHI); età; fascia retributiva; data di nascita; livello di istruzione; indirizzo e-mail; ID dipendente/Customer Employment ID; nome del datore di lavoro; storia o stato occupazionale; indicatore di famiglia con figli; genere; nome della persona fisica (cognome + nome/iniziale); polizze assicurative; tipologia di congedo; stato civile o di famiglia; occupazione; data di pensionamento; data di cessazione; indirizzo; codice fiscale; telefono/cellulare personale/fax; username
Per garantire la sicurezza della rete, degli uffici e dei dati, anche con l'obiettivo di impedire accessi non autorizzati ai sistemi e alle sedi di American Express,	Dati biometrici; fascia retributiva; indirizzo e-mail; ID dipendente/Customer Employment ID; ID dipendente/ID cliente a fini lavorativi; fotografia

Tipologia di trattamento e finalità	Categorie di Dati personali
tutelare i dipendenti, gli interessi commerciali e le proprietà della società, e prevenire le frodi, anche facilitando l'accesso e il monitoraggio delle attività svolte nelle sedi e sui sistemi American Express oltre che della conformità alle policy interne.	
Per finalità o requisiti di formazione, istruzione e sviluppo, compresa la creazione di un profilo dipendente per facilitare tali attività.	Fascia retributiva; indirizzo e-mail; dati app/dispositivo; ID dipendente/Customer Employment ID; nome del datore di lavoro; indirizzo IP; nome della persona fisica (cognome + nome/iniziale)
Per verificare le credenziali dei Dipendenti relative all'istruzione (es. ottenimento di una qualifica o certificazione nel corso del rapporto di lavoro con American Express).	Nome della persona fisica (cognome + nome/iniziale); storia o stato occupazionale; data di nascita
Per finalità aziendali interne e di gestione, anche con l'obiettivo di garantire la conformità alle policy interne di American Express, oltre ad attività di budgeting, forecast, planning e relative analisi e gestione (inclusa l'elaborazione di report di analisi, anche aggregati e resi anonimi).	numero di conto (completo/parziale/criptato) - AMEX
Per gestire, amministrare e/o riorganizzare le attività, gli asset e le operazioni American Express (anche in previsione di eventuali vendite, fusioni o cessioni aziendali).	Fascia retributiva; dati sulla diversità; indirizzo e-mail; ID dipendente/Customer Employment ID; storia o stato occupazionale; genere; nome della persona fisica (cognome + nome/iniziale); indirizzo IP; occupazione; opinioni raccolte; valutazione delle prestazioni; data di cessazione
Per trasmettere informazioni e gestire le policy aziendali interne, l'utilizzo degli uffici e il nostro patrimonio immobiliare, e per migliorare le condizioni di lavoro dei dipendenti (inclusa	ID dipendente/Customer Employment ID; nome della persona fisica (cognome + nome/iniziale); indirizzo e-mail; fascia retributiva; nome del datore di lavoro

Tipologia di trattamento e finalità	Categorie di Dati personali
l'elaborazione di report di analisi, anche aggregati e resi anonimi).	
Per registrare e monitorare le chiamate con i clienti con le seguenti finalità: formazione, qualità, conformità, prevenzione delle frodi e gestione dei reclami.	Numero di conto (completo/parziale/criptato) - Altri istituti di pagamento; Carta di Identità; PIN/codice di accesso/password; numero di previdenza sociale (completo/parziale/criptato); reddito; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); data di scadenza della carta di credito; dati relativi a transazioni/acquisti da parte del cliente; data di nascita; indirizzo e-mail; nome della persona fisica (cognome + nome/iniziale); indirizzo; telefono/cellulare personale/fax
Per finalità contabili e di audit.	Reddito; età; fascia retributiva; data di nascita; ID dipendente/Customer Employment ID; nome del datore di lavoro; storia o stato occupazionale; nome della persona fisica (cognome + nome/iniziale); data di pensionamento; data di cessazione
Per garantire pari opportunità e parità di trattamento in conformità alle policy e la legislazione sulle pari opportunità, e per le iniziative in ambito di diversità, uguaglianza e inclusione a livello globale.	Origine etnica; età; fascia retributiva; data di nascita; dati sulla diversità; indirizzo e-mail; ID dipendente/Customer Employment ID; nome del datore di lavoro; genere; nome della persona fisica (cognome + nome/iniziale); occupazione
Per gestire e analizzare le spese aziendali e dei dipendenti e per gestire gli strumenti tecnologici (es. gestione dei dispositivi American Express).	Numero di conto (completo/parziale/criptato) - AMEX; numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento; indirizzo e-mail; ID dipendente/Customer Employment ID; nome della persona fisica (cognome + nome/iniziale); indirizzo; codice fiscale
Per ottemperare alle leggi in vigore e svolgere attività di sanctions screening, anche laddove richiesto in relazione a provvedimenti giudiziari o amministrativi riguardanti	Nazionalità; numero di conto (completo/parziale/criptato) - AMEX; numero di patente di guida; numero di Green card/Alien resident card; Carta di Identità; numero di passaporto; numero di previdenza sociale (completo/parziale/criptato); informazioni

Tipologia di trattamento e finalità	Categorie di Dati personali
singoli dipendenti e/o per presentare documentazione regolatoria e/o per condurre indagini interne.	sull'agente autorizzato/sulla gestione del programma; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); dati relativi a transazioni/acquisti da parte del cliente; data di nascita; indirizzo e-mail; nome del datore di lavoro; genere; nome della persona fisica (cognome + nome/iniziale); indirizzo IP; Non-driver's ID; occupazione; storico dei pagamenti; dati aziendali del lavoratore autonomo/proprietario; dati anagrafici del lavoratore autonomo/proprietario; indirizzo; codice fiscale; telefono/cellulare personale/fax; età; record locator di biglietti o viaggi; affiliazioni/opinioni politiche; cognome da nubile della madre
Per collaborare con le autorità (di regolamentazione, preposte all'applicazione della legge, ecc.).	Nome della persona fisica (cognome + nome/iniziale); fascia retributiva; ID dipendente/Customer Employment ID; indirizzo e-mail; telefono/cellulare personale/fax; indirizzo; altro (specificare)
Per commercializzare e inviare promozioni e offerte sui prodotti, servizi e incentivi per i dipendenti di American Express.	Fascia retributiva; dati sulla diversità; indirizzo e-mail; solo per i dirigenti - ID dipendente/Customer Employment ID; storia o stato occupazionale; genere; nome della persona fisica (cognome + nome/iniziale); solo per i dirigenti; indirizzo IP; occupazione; opinioni raccolte; valutazione delle prestazioni; data di cessazione
Per monitorare ed elaborare report relativi alla diversità dell'ambiente di lavoro e per sviluppare iniziative volte a promuovere un ambiente di lavoro più inclusivo, American Express può trattare i dati personali relativi all'orientamento sessuale o alla condizione di disabilità dei dipendenti.	Origine etnica; età; fascia retributiva; data di nascita; dati sulla diversità; indirizzo e-mail; ID dipendente/Customer Employment ID; nome del datore di lavoro; genere; nome della persona fisica (cognome + nome/iniziale); occupazione
Dati biometrici per identificare il dipendente e consentire l'accesso agli uffici.	Dati biometrici; fascia retributiva; indirizzo e-mail; ID dipendente/Customer Employment ID; nome della persona fisica (cognome + nome/iniziale); fotografia

Tipologia di trattamento e finalità	Categorie di Dati personali
Per rispettare le legislazioni in materia di salute e sicurezza e di pari opportunità, American Express può trattare dati personali relativi alla salute o alla condizione dei dipendenti (es. informazioni relative a eventuali disabilità).	Informazioni sanitarie protette (PHI); ID dipendente/Customer Employment ID; nome della persona fisica (cognome + nome/iniziale); indirizzo e-mail; fascia retributiva; nome del datore di lavoro
American Express può trattare dati personali relativi alla salute o alla condizione dei dipendenti nell'ambito della gestione delle assenze per malattia o degli infortuni sul lavoro, per amministrare i benefit e per assicurarsi di garantire ai dipendenti i giusti diritti e il giusto supporto.	Numero di conto (completo/parziale/criptato) - Altri istituti di pagamento; numero di patente di guida; Carta di Identità; numero di previdenza sociale (completo/parziale/attestato); informazioni sui figli (età/genere, informazioni di contatto, ecc.); disabilità / alloggio su base normativa; reddito; nazionalità; informazioni sanitarie protette (PHI); età; fascia retributiva; data di nascita; livello di istruzione; indirizzo e-mail; ID dipendente/Customer Employment ID; nome del datore di lavoro; storia o stato occupazionale; indicatore di famiglia con figli; genere; nome della persona fisica (cognome + nome/iniziale); polizze assicurative; tipologia di congedo; stato civile o di famiglia; occupazione; data di pensionamento; data di cessazione; indirizzo; codice fiscale; telefono/cellulare personale/fax; username
American Express può trattare dati personali relativi a condanne penali e reati in determinate circostanze, comprese situazioni in cui sussiste l'obbligo giuridico di rispondere alle richieste delle forze dell'ordine, attività di sanctions screening e nel contesto di azioni legali che generano la necessità, per la società, di accettare, esercitare o difendere i propri diritti legali.	Nome della persona fisica (cognome + nome/iniziale); storia o stato occupazionale; altro (specificare); data di nascita
Categorie di Interessati: Clienti	
Per evadere le richieste relative a carte, conti o altri prodotti o per	Data di nascita; indirizzo e-mail; nome della persona fisica (cognome + nome/iniziale); nazionalità;

Tipologia di trattamento e finalità	Categorie di Dati personali
gestire i conti esistenti di un cliente.	telefono/cellulare personale/fax; cognome da nubile della madre; numero di passaporto
Per segnalare particolari transazioni sospette alle autorità competenti ai sensi delle norme antiriciclaggio o, come previsto dalla legge, per svolgere attività di due diligence dei Clienti prima di approvarne le richieste.	Numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento; numero di conto (completo/parziale/criptato) - Altri istituti di pagamento; numero di conto (completo/parziale/criptato) - AMEX; numero di patente di guida; numero di Green card/Alien resident card; Carta di Identità; numero di passaporto; numero di previdenza sociale (completo/parziale/criptato); precedenti penali; reddito; sentenze o procedimenti giudiziari; iscrizione a sindacati o associazioni; nazionalità; età; altro (specificare); fascia retributiva; tipo di Carta (es. codice goffrato) / codice di servizio (parametri della carta); dati ROC relativi ai contributi di beneficenza; data di scadenza della Carta; dati relativi a transazioni/acquisti da parte del cliente; Customer service record; stato cliente; data di nascita; livello di istruzione; affiliazioni accademiche o professionali; indirizzo e-mail; badge/foto profilo del dipendente; ID dipendente/Customer Employment ID; nome del datore di lavoro; storia o stato occupazionale; genere; nome della persona fisica (cognome + nome/iniziale); indirizzo IP; numero del conto Membership Rewards®(MR); cognome da nubile della madre; Non-driver's ID; occupazione; storico dei pagamenti; valutazione delle prestazioni; dati personali di directory; fotografia; dati ROC (Records of Charge) relativi a servizi finanziari/governativi/sanitari; indirizzo; codice fiscale; telefono/cellulare personale/fax; numero del biglietto o record locator del viaggio
Per adempiere ai nostri obblighi normativi in fase di analisi della richiesta del cliente.	Numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento; numero di conto (completo/parziale/criptato) - AMEX; numero di patente di guida; Carta di Identità; numero di passaporto; numero di previdenza sociale (completo/parziale/criptato); reddito; età; stato cliente; data di nascita; indirizzo e-mail; nome del datore di lavoro; esito attività di credit scoring;

Tipologia di trattamento e finalità	Categorie di Dati personali
	genere; nome della persona fisica (cognome + nome/iniziale); cognome da nubile della madre; occupazione; storico dei pagamenti; indirizzo; codice fiscale; telefono/cellulare personale/fax
Per amministrare e gestire il conto del cliente e fornire a quest'ultimo e/o alla sua azienda i servizi American Express, es. elaborare, approvare e completare singole transazioni.	Numero di conto (completo/parziale/criptato) - AMEX; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); indirizzo e-mail; nome della persona fisica (cognome + nome/iniziale); numero di patente di guida; Carta di Identità; PIN/codice di accesso/password; reddito; sentenze o procedimenti giudiziari; età; data di scadenza della carta di credito; data di nascita; nome del datore di lavoro; storia o stato occupazionale; esito attività di credit scoring; dati aziendali del lavoratore autonomo/proprietario; indirizzo; codice fiscale; telefono/cellulare personale/fax; domanda e/o risposte di sicurezza / verifica; identificativo univoco online (compresi cookie); dati relativi a transazioni/acquisti da parte del cliente; preferenze di privacy e marketing (es. DNC); occupazione; P(P1); informazioni sull'agente autorizzato/sulla gestione del programma; stato cliente; Customer service record; High value Card Member indicator; polizze assicurative; stato civile o di famiglia; numero del conto Membership Rewards®(MR); storico dei pagamenti; dati ROC (Records of Charge) relativi a servizi finanziari/governativi/sanitari; dati anagrafici del lavoratore autonomo/proprietario; username; Customer service record; stato cliente; cognome da nubile della madre; numero del conto partner (incl. numero FF)
Per gestire benefit, assicurazioni, viaggi o altri programmi aziendali a cui il cliente o la sua azienda è iscritto	Numero di conto (completo/parziale/criptato) - AMEX; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); data di scadenza della carta di credito; dati relativi a transazioni/acquisti da parte del cliente; Customer service record; stato cliente; data di nascita; indirizzo e-mail; High value Card Member indicator; preferenze di privacy e marketing (es. DNC); numero del conto Membership

Tipologia di trattamento e finalità	Categorie di Dati personali
	Rewards®(MR) cognome da nubile della madre; numero del conto partner (incl. numero FF); indirizzo; telefono/cellulare personale/fax; username
Per fornire ai clienti i servizi location-based richiesti (se del caso)	Numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento; Carta di Identità; età; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); data di scadenza della carta di credito; stato cliente; data di nascita; indirizzo e-mail; genere; High value Card Member indicator; nome della persona fisica (cognome + nome/iniziale); numero del conto partner (incl. numero FF); indirizzo; telefono/cellulare personale/fax; Token/GUID/PAR
Per comunicare con i clienti tramite e-mail, SMS o qualsiasi altro mezzo elettronico, oppure tramite posta e/o telefono, in merito ai relativi conti, prodotti e servizi per finalità legali, normative o di assistenza (es. per fornire aggiornamenti sulle caratteristiche dei prodotti o servizi del cliente).	Numero di conto (completo/parziale/criptato) - AMEX; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); telefono/cellulare personale/fax; numero del biglietto o record locator del viaggio; età; dati relativi a transazioni/acquisti da parte del cliente; data di nascita; disabilità / alloggio su base normativa; dati sulla diversità; livello di istruzione; indirizzo e-mail; nome del datore di lavoro; storia o stato occupazionale; indicatore di famiglia con figli; esito attività di credit scoring; genere; High value Card Member indicator indicator; reddito; nome della persona fisica (cognome + nome/iniziale); indirizzo IP; stato civile o di famiglia; occupazione; identificativo univoco online (compresi cookie); opinioni raccolte; fotografia; informazioni in tempo reale/precise/di geo-localizzazione; orientamento sessuale; indirizzo; Carta di Identità; informazioni sull'agente autorizzato/sulla gestione del programma; data di scadenza della carta di credito; stato cliente; Customer service record; polizze assicurative; stato civile o di famiglia; preferenze di privacy e marketing (es. DNC); numero del conto Membership Rewards®(MR); altro (specificare); storico dei pagamenti; dati ROC (Records of Charge) relativi a servizi finanziari/governativi/sanitari; dati aziendali del lavoratore autonomo/proprietario; dati anagrafici del

Tipologia di trattamento e finalità	Categorie di Dati personali
	lavoratore autonomo/proprietario; codice fiscale; username
Per fornire un servizio appropriato e/o tutelare gli interessi dei clienti apportando ragionevoli modifiche, ad esempio inviando o fornendo informazioni in un formato idoneo.	Numero di conto (completo/parziale/criptato) - AMEX; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); indirizzo e-mail; nome della persona fisica (cognome + nome/iniziale); numero di patente di guida; Carta di Identità; PIN/codice di accesso/password; reddito; sentenze o procedimenti giudiziari; età; data di scadenza della carta di credito; data di nascita; nome del datore di lavoro; storia o stato occupazionale; esito attività di credit scoring; dati aziendali del lavoratore autonomo/proprietario; indirizzo; codice fiscale; telefono/cellulare personale/fax; domanda e/o risposte di sicurezza / verifica; identificativo univoco online (compresi cookie); dati relativi a transazioni/acquisti da parte del cliente; preferenze di privacy e marketing (es. DNC); occupazione; P(P1); informazioni sull'agente autorizzato/sulla gestione del programma; stato cliente; Customer service record; High value Card Member indicator; polizze assicurative; stato civile o di famiglia; numero del conto Membership Rewards®(MR) ; storico dei pagamenti; dati ROC (Records of Charge) relativi a servizi finanziari/governativi/sanitari; dati anagrafici del lavoratore autonomo/proprietario; username; Customer service record; stato cliente; cognome da nubile della madre; numero del conto partner (incl. numero FF)
Per fornire assistenza e gestire eventuali benefit e programmi assicurativi erogati unitamente ai prodotti o ai servizi richiesti dal cliente	Numero di conto (completo/parziale/criptato) - AMEX; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); data di scadenza della carta di credito; dati relativi a transazioni/acquisti da parte del cliente; Customer service record; stato cliente; data di nascita; indirizzo e-mail; High value Card Member indicator; preferenze di privacy e marketing (es. DNC); numero del conto Membership Rewards®(MR); cognome da nubile della

Tipologia di trattamento e finalità	Categorie di Dati personali
	madre; numero del conto partner (incl. numero FF); indirizzo; telefono/cellulare personale/fax; username
In caso di interazione con alcuni dei partner commerciali di American Express in relazione ai benefici della carta, per connettere, per connettere il cliente al proprio account Membership Rewards (se del caso) e, a seconda del prodotto, consentire l'utilizzo dei punti Membership Rewards per pagare prodotti o servizi di un partner	numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento
Per effettuare controlli con l'obiettivo di garantire la sicurezza del conto e dei dati personali di un cliente, individuare e prevenire frodi o attività criminali (compresa la revisione e l'approvazione di singole transazioni) e verificare l'identità del cliente prima di erogare servizi (anche attraverso il processo di screening e monitoraggio "know your customer").	numero di conto (completo/parziale/criptato) - AMEX; numero di previdenza sociale (completo/parziale/criptato); numero di patente di guida; Carta di Identità; informazioni sull'agente autorizzato/sulla gestione del programma; data di nascita; indirizzo e-mail; nome della persona fisica (cognome + nome/iniziale); codice fiscale
Per rispondere alle domande che il cliente pone ad American Express, rispondere alle sue richieste e gestire eventuali reclami da parte del cliente stesso.	Numero di conto (completo/parziale/criptato) - AMEX; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); indirizzo e-mail; nome della persona fisica (cognome + nome/iniziale); numero di patente di guida; Carta di Identità; PIN/codice di accesso/password; reddito; sentenze o procedimenti giudiziari; età; data di scadenza della carta di credito; data di nascita; nome del datore di lavoro; storia o stato occupazionale; esito attività di credit scoring; dati aziendali del lavoratore autonomo/proprietario; indirizzo; codice fiscale; telefono/cellulare personale/fax; domanda e/o risposte di sicurezza / verifica; identificativo univoco online (compresi cookie); dati relativi a transazioni/acquisti da parte del cliente; preferenze

Tipologia di trattamento e finalità	Categorie di Dati personali
	di privacy e marketing (es. DNC); occupazione; P(P1); informazioni sull'agente autorizzato/sulla gestione del programma; stato cliente; Customer service record; High value Card Member indicator; polizze assicurative; stato civile o di famiglia; numero del conto Membership Rewards®(MR); storico dei pagamenti; dati ROC (Records of Charge) relativi a servizi finanziari/governativi/sanitari; dati anagrafici del lavoratore autonomo/proprietario; username; Customer service record; stato cliente; cognome da nubile della madre; numero del conto partner (incl. numero FF)
Per tutelare gli interessi commerciali di American Express, recuperare i crediti ed esercitare altri diritti derivanti da qualsiasi contratto in essere con il Cliente.	Numero di conto (completo/parziale/criptato) - AMEX; domanda e/o risposte di sicurezza / verifica; numero di patente di guida; Carta di Identità; PIN/codice di accesso/password; reddito; sentenze o procedimenti giudiziari; età; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); data di scadenza della carta di credito; data di nascita; indirizzo e-mail; nome del datore di lavoro; storia o stato occupazionale; esito attività di credit scoring; nome della persona fisica (cognome + nome/iniziale); dati aziendali del lavoratore autonomo/proprietario; indirizzo; codice fiscale; telefono/cellulare personale/fax; numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento; dati relativi a transazioni/acquisti da parte del cliente; genere; High value Card Member indicator; occupazione; storico dei pagamenti; algoritmi proprietari predittivi del credit score e relativi alla proprietà intellettuale
Per istituire, esercitare o difendere diritti o rivendicazioni legali e fornire assistenza nella risoluzione delle controversie.	Nome della persona fisica (cognome + nome/iniziale); fascia retributiva; ID dipendente/Customer Employment ID; indirizzo e-mail; telefono/cellulare personale/fax; indirizzo; altro (specificare)
Per sviluppare e migliorare i prodotti e servizi American	Numero di conto (completo/parziale/criptato) - AMEX; dati relativi a transazioni/acquisti da parte del

Tipologia di trattamento e finalità	Categorie di Dati personali
Express, anche con l'obiettivo di comprendere meglio i clienti, le loro esigenze, preferenze e comportamenti; per raggruppare i clienti che mostrano analogie per offrire prodotti o servizi particolarmente idonei o adatti alle loro preferenze; per valutare e analizzare l'efficacia di annunci, promozioni e offerte di American Express.	cliente; High value Card Member indicator; nome della persona fisica (cognome + nome/iniziale)
Per consentire ad American Express di comprendere meglio la situazione finanziaria e il comportamento dei clienti in modo da poter prendere decisioni in merito alla gestione dei conti esistenti e stabilire quali altri prodotti o servizi possano essere offerti.	Numero di conto (completo/parziale/criptato) - AMEX; dati relativi a transazioni/acquisti da parte del cliente; esito attività di credit scoring; algoritmi proprietari predittivi del credit score e relativi alla proprietà intellettuale; reddito; età; informazioni sul mutuo o su altri prestiti; storico dei pagamenti
Per verificare la corretta esecuzione delle istruzioni dei clienti; per sviluppare e migliorare i servizi American Express; per finalità formative e di qualità.	Informazioni sui figli (età/genere, informazioni di contatto, ecc.); disabilità / alloggio su base normativa; numero di conto (completo/parziale/criptato) - AMEX; nazionalità; età; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); data di nascita; telefono/cellulare personale/fax; indirizzo e-mail; domanda e/o risposte di sicurezza / verifica; numero di passaporto; informazioni sanitarie protette (PHI); informazioni sull'agente autorizzato/sulla gestione del programma; data di scadenza della carta di credito; genere; nome della persona fisica (cognome + nome/iniziale); indirizzo; numero del biglietto o record locator del viaggio; Carta di Identità; data di scadenza della carta di credito; dati relativi a transazioni/acquisti da parte del cliente; stato cliente; Customer service record; High value Card Member indicator; polizze assicurative; stato civile o di famiglia; preferenze di privacy e marketing (es. DNC); numero del conto

Tipologia di trattamento e finalità	Categorie di Dati personali
	Membership Rewards®(MR); occupazione; storico dei pagamenti; dati ROC (Records of Charge) relativi a servizi finanziari/governativi/sanitari; dati aziendali del lavoratore autonomo/proprietario; dati anagrafici del lavoratore autonomo/proprietario; codice fiscale; username; ID dipendente/Customer Employment ID; telefono/cellulare personale/fax; cognome da nubile della madre; numero del conto partner (incl. numero FF)
Per registrare e monitorare le chiamate con i clienti con le seguenti finalità: formazione, qualità, conformità, prevenzione delle frodi e gestione dei reclami.	Domanda e/o risposte di sicurezza / verifica; numero di patente di guida; numero di passaporto; informazioni sui figli (età/genere, informazioni di contatto, ecc.); disabilità / alloggio su base normativa; nazionalità; informazioni sanitarie protette (PHI); età; informazioni sull'agente autorizzato/sulla gestione del programma; genere; numero del biglietto o record locator del viaggio; numero di conto (completo/parziale/criptato) - AMEX; numero di conto (completo/parziale/criptato) - Altri istituti di pagamento; Carta di Identità; PIN/codice di accesso/password; numero di previdenza sociale (completo/parziale/criptato); reddito; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); data di scadenza della carta di credito; dati relativi a transazioni/acquisti da parte del cliente; data di nascita; indirizzo e-mail; nome della persona fisica (cognome + nome/iniziale); indirizzo; telefono/cellulare personale/fax
Per specifiche finalità relative all'Open Banking.	Numero di conto (completo/parziale/criptato) - AMEX; numero di conto (completo/parziale/criptato); Altri istituti di pagamento; nome della persona fisica (cognome + nome/iniziale); dati relativi a transazioni/acquisti da parte del cliente
Per condurre test (per garantire la sicurezza e durante la fase di aggiornamento dei sistemi	PIN/codice di accesso/password; dati app/dispositivo; indirizzo e-mail; telefono/cellulare personale/fax; ID dipendente/Customer

Tipologia di trattamento e finalità	Categorie di Dati personali
American Express), per gestire attività inerenti all'amministrazione del sito web e al supporto e sviluppo del sistema informatico e per salvaguardare la sicurezza dei Dati personali dei clienti.	Employment ID; Token/GUID/PAR; username; indirizzo IP
Per sviluppare e perfezionare le policy, i modelli e le procedure di American Express in materia di gestione del rischio per le richieste e i conti dei clienti, sulla base delle informazioni contenute nella richiesta o relative alla solvibilità dei clienti (comprese le informazioni fornite da terzi), al rischio di frode e alla storia del conto (se del caso).	Numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento; numero di conto (completo/parziale/criptato) - AMEX; numero di patente di guida; Carta di Identità; numero di passaporto; numero di previdenza sociale (completo/parziale/criptato); reddito; età; stato cliente; data di nascita; indirizzo e-mail; nome del datore di lavoro; esito attività di credit scoring; genere; nome della persona fisica (cognome + nome/iniziale); cognome da nubile della madre; occupazione; storico dei pagamenti; indirizzo; codice fiscale; telefono/cellulare personale/fax
Per le attività di recupero crediti e per condividere informazioni con agenzie di recupero crediti e di gestione delle frodi.	Numero di conto (completo/parziale/criptato) - AMEX; domanda e/o risposte di sicurezza / verifica; Carta di Identità; PIN/codice di accesso/password; numero di previdenza sociale (completo/parziale/criptato); reddito; sentenze o procedimenti giudiziari; ricezione di assegni di mantenimento per i figli, alimenti o mantenimento separato; ricezione di assistenza statale (es. sussidi statali); età; tipo di carta (es. codice cifrato) / codice di servizio (parametri della carta); data di scadenza della carta di credito; codice di sicurezza della carta di credito; dati relativi a transazioni/acquisti da parte del cliente; stato cliente; data di nascita; indirizzo e-mail; nome del datore di lavoro; esito attività di credit scoring
Per condurre ricerche e analisi, incl. consentire al cliente di fornire un feedback valutando e recensendo i prodotti e servizi American Express e quelli dei partner commerciali della	Numero di conto (completo/parziale/criptato) - AMEX; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); dati relativi a transazioni/acquisti da parte del cliente; indirizzo e-mail; storico dei pagamenti; username

Tipologia di trattamento e finalità	Categorie di Dati personali
società, e per condurre attività di data analytics, ricerche statistiche e report aggregati.	
Per elaborare report e statistiche al fine di consentire alla società del cliente di mantenere una politica efficace in termini di amministrazione e procurement (può includere anche informazioni relative a debiti insoluti).	Nome della persona fisica (cognome + nome/iniziale); data di nascita; nazionalità; occupazione; telefono/cellulare personale/fax; indirizzo e-mail; indirizzo
Per collaborare con le autorità (di regolamentazione, preposte all'applicazione della legge, ecc.).	Fascia retributiva; domanda e/o risposte di sicurezza / verifica; identificativo univoco online (compresi cookie); PIN/codice di accesso/password; informazioni in tempo reale/precise/di geolocalizzazione; dati TRACK; data di scadenza della carta di credito; dati relativi a transazioni/acquisti da parte del cliente; storico dei pagamenti; dati ROC (Records of Charge) relativi a servizi finanziari/governativi/sanitari; genere; luogo di nascita; numero di conto (completo/parziale/criptato) - AMEX; numero di patente di guida; numero di Green card/Alien resident card; Carta di Identità; numero di passaporto; numero di previdenza sociale (completo/parziale/criptato); reddito; nazionalità; informazioni sull'agente autorizzato/sulla gestione del programma; stato cliente (di default); stato cliente; data di nascita; indirizzo e-mail; ID dipendente/Customer Employment ID; nome del datore di lavoro; storia o stato occupazionale; nome della persona fisica (cognome + nome/iniziale); indirizzo IP; Non-driver's ID; occupazione; dati aziendali del lavoratore autonomo/proprietario; dati anagrafici del lavoratore autonomo/proprietario; indirizzo; codice fiscale; telefono/cellulare personale/fax
Per adempiere agli obblighi legali e normativi (es. esecuzione dei controlli di due diligence del	Numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento; numero di conto (completo/parziale/criptato) - AMEX; numero di patente di guida; Carta di Identità; numero di

Tipologia di trattamento e finalità	Categorie di Dati personali
cliente prima di approvarne la richiesta).	passaporto; PIN/codice di accesso/password; reddito; nazionalità; età; patrimonio netto; informazioni sull'agente autorizzato/sulla gestione del programma; tipo di carta (es. codice goffrato); stato cliente; data di nascita; dati app/dispositivo; livello di istruzione; affiliazioni accademiche o professionali; indirizzo e-mail; nome del datore di lavoro; storia o stato occupazionale; nome della persona fisica (cognome + nome/iniziale); indirizzo IP; preferenze di privacy e marketing (es. DNC) numero del conto Membership Rewards®(MR); informazioni sul mutuo o su altri prestiti; Non-driver's ID; occupazione; altro documento d'identità rilasciato dal governo; numero del conto partner (incl. numero FF); algoritmi proprietari predittivi del credit score e relativi alla proprietà intellettuale; dati aziendali del lavoratore autonomo/proprietario; dati anagrafici del lavoratore autonomo/proprietario; indirizzo; telefono/cellulare personale/fax
Per commercializzare prodotti e servizi che American Express ritiene possano interessare al cliente in base al rapporto che intercorre con la società (tramite e-mail, SMS o telefono - es. in caso di telefonata da parte del cliente). American Express procederà in tal senso esclusivamente nei casi consentiti dalla legge tenendo in considerazione eventuali opt-out.	Numero di conto (completo/parziale/criptato) - AMEX; altro (specificare); età; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); dati relativi a transazioni/acquisti da parte del cliente; data di nascita; disabilità / alloggio su base normativa; dati sulla diversità; livello di istruzione; indirizzo e-mail; nome del datore di lavoro; storia o stato occupazionale; indicatore di famiglia con figli; esito attività di credit scoring; genere; High value Card Member indicator; reddito; nome della persona fisica (cognome + nome/iniziale); indirizzo IP; stato civile o di famiglia; occupazione; identificativo univoco online (compresi cookie); opinioni raccolte; fotografia; informazioni in tempo reale/precise/di geo-localizzazione; orientamento sessuale; indirizzo; telefono/cellulare personale/fax
Per pubblicizzare, commercializzare e inviare ai clienti promozioni e offerte relative a prodotti e servizi per o da parte del Gruppo American	Numero di conto (completo/parziale/criptato) - Altri istituti non di pagamento; Carta di Identità; età; tipo di carta (es. codice goffrato) / codice di servizio (parametri della carta); data di scadenza della carta di credito; stato cliente; data di nascita; indirizzo e-

Tipologia di trattamento e finalità	Categorie di Dati personali
<p>Express (ovvero qualsiasi affiliata, sussidiaria, joint venture e qualsiasi società posseduta o controllata dalla società controllante) e dei partner commerciali della società, compresa la presentazione di contenuti personalizzati, e in linea con le preferenze e gli interessi dei clienti, tra cui pubblicità mirata su più dispositivi o mostrando offerte nella sezione Manage Your Card Account (MYCA).</p>	<p>mail; genere; High value Card Member indicator; nome della persona fisica (cognome + nome/iniziale); numero del conto partner (incl. numero FF); indirizzo; telefono/cellulare personale/fax; Token/GUID/PAR</p>
<p>Dati biometrici per identificare il cliente, per verifiche di sicurezza e per individuare e prevenire le frodi.</p>	<p>Dati biometrici; fotografia</p>

APPENDICE 2 - SOCIETÀ DEL GRUPPO AMERICAN EXPRESS VINCOLATE ALLE BCR

Entità giuridiche BCR a luglio 2024						
Ragione sociale	Paese	Indirizzo della sede centrale	Tipologia di entità	Attività principale	Importatore / Esportatore	Identificativa società
American Express (India) Private Limited	India	MGF Metropolitan - Saket, 7th Floor, Office Block, District Centre Saket, New Delhi, 110017, India	Controllata di maggioranza o al 100%	Fornisce servizi di supporto per altre società Amex	Importatore di dati / Esportatore di dati	U74899DL1994PTC059865
American Express (Malaysia) SDN. BHD.	Malesia	Level 14, Menara Prestige, No.1, Jalan Pinang, 50450 Kuala Lumpur, Malesia	Controllata di maggioranza o al 100%	Società di servizi al cliente	Importatore di dati / Esportatore di dati	46752-M
American Express (Thai) Company Limited	Thailandia	S.P. Building, 388 Phaholyothin Road, Samsennai, Phayathai, Bangkok, 10400, Thailandia	Controllata di maggioranza o al 100%	Emissione di carte di credito e carte di credito a saldo	Importatore di dati / Esportatore di dati	105524019341.00
American Express Argentina S.A.	Argentina	Arenales 707, Mezzanine, Ciudad de Buenos Aires, Buenos Aires, C1061AAA, Argentina	Controllata di maggioranza o al 100%	Emissione di carte di credito e carte di credito a saldo	Importatore di dati / Esportatore di dati	161972

American Express Australia Limited	Australia	Level 1, 12 Shelley Street, Sydney NSW 2000, Australia	Controllata di maggioranza o al 100%	Società di servizi d'affari	Importatore / Esportatore di dati	108 952 085
American Express Business Solutions (India) Private Limited	India	MGF Metropolitan - Saket, 7th Floor, Office Block, District Centre Saket, New Delhi, 110017, India	Controllata di maggioranza o al 100%	Società di servizi al cliente	Importatore / Esportatore di dati	U74140DL2015PTC27/109
American Express Carte France SA	Francia	Bâtiment, Voyager, 8-10 rue Henri, Sainte Claire Deville, 92500, Rueil Malmaison, Francia	Controllata di maggioranza o al 100%	Emissione di carte di credito e/o carte di credito a saldo	Esportatore di dati	313 536 898 00015
American Express Company	Stati Uniti	200 Vesey Street, New York NY 10285, Stati Uniti	Società controllante	Società di merchant acquisition/servizi d'affari	Importatore / Esportatore di dati	13-4922250
American Express Company (Mexico) S.A. de C.V.	Messico	Avenida Patriotismo #635, Col. Ciudad de los Deportes, Mexico City, Messico, 03710, Messico	Controllata di maggioranza o al 100%	Emissione di carte di credito a saldo	Importatore / Esportatore di dati	AEC810901298
American Express Credit Corporation	Stati Uniti	200 Vesey Street, New York NY 10285, Stati Uniti	Controllata di maggioranza o al 100%	Società di finanziamento dei crediti delle carte di credito a saldo	Importatore / Esportatore di dati	11-1988350

American Express de Espana, S.A. (Sociedad Unipersonal)	Spagna	Avda. Partenón 12-14, 28042, Madrid, Spagna	Controllata di maggioranza o al 100%	Elaborazione dei pagamenti con carta di credito	Esportatore di dati	A-28521888
American Express Europe LLC	Stati Uniti	200 Vesey Street, New York NY 10285, Stati Uniti	Controllata di maggioranza o al 100%	Servizi connessi ai viaggi	Importatore di dati / Esportatore di dati	13-3147632
American Express Europe LLC - Filiale - Regno Unito	Regno Unito	200 Vesey Street, New York NY 10285, Stati Uniti	Filiale	Servizi di cambio valuta	Importatore di dati / Esportatore di dati	BR000897
American Express Europe, S.A.	Spagna	Avda. Partenón 12-14, 28042, Madrid, Spagna	Controllata di maggioranza o al 100%	Emissione di carte di credito e carte di credito a saldo	Esportatore di dati	A-82628041
American Express Europe, S.A. - Filiale - Austria	Austria	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte	Esportatore di dati	FN 495241 x
American Express Europe, S.A. - Filiale - Belgio	Belgio	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Servizi finanziari e altre attività correlate	Esportatore di dati	0776.653.759
American Express Europe, S.A. - Filiale - Danimarca	Danimarca	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte di credito a saldo	Esportatore di dati	39560542
American Express Europe, S.A. - Filiale - Finlandia	Finlandia	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte di credito a saldo e servizi Travel & Lifestyle	Esportatore di dati	2914I39-2
American Express Europe, S.A. - Filiale - Germania	Germania	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte di credito e carte di credito a saldo	Esportatore di dati	HRB 112342

American Express Europe, S.A. - Filiale - Ungheria	Ungheria	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte di credito e carte di credito a saldo	Esportatore di dati	Non disponibile
American Express Europe, S.A. - Filiale - Irlanda	Irlanda	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte	Esportatore di dati	908882
American Express Europe, S.A. - Filiale - Paesi Bassi	Paesi Bassi	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte	Esportatore di dati	71660275
American Express Europe, S.A. - Filiale - Norvegia	Norvegia	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte di credito a saldo e servizi Travel & Lifestyle	Esportatore di dati	920 854 346
American Express Europe, S.A. - Filiale - Polonia	Polonia	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte di credito e carte di credito a saldo	Esportatore di dati	KRS 0000733504
American Express Europe, S.A. - Filiale - Svezia	Svezia	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Emissione di carte di credito a saldo e servizi Travel & Lifestyle	Esportatore di dati	516411-3911
American Express Group Services Limited	Regno Unito	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, Regno Unito	Controllata di maggioranza o al 100%	Ufficio amministrativo	Importatore di dati / Esportatore di dati	6613927
American Express Innovation Laboratories Limited - Filiale - Singapore	Singapore	70 Sir John Rogerson'S Quay, Dublin 2, Irlanda	Filiale	Sviluppo di software e applicazioni	Importatore di dati / Esportatore di dati	T22FC0063A

American Express Insurance Services, Agente de Seguros, S.A. de C.V.	Messico	Avenida Patriotismo #635, Col. Ciudad de los Deportes, Mexico City, Messico, 03710, Messico	Controllata di maggioranza o al 100%	Broker o agente assicurativo	Importatore di dati / Esportatore di dati	Non applicabile
American Express International (NZ), Inc.	Stati Uniti	200 Vesey Street, New York NY 10285, Stati Uniti	Controllata di maggioranza o al 100%	Società di merchant acquisition e servizi d'affari	Importatore di dati / Esportatore di dati	22-2155644
American Express International (NZ), Inc. - Filiale - Nuova Zelanda	Nuova Zelanda	200 Vesey Street, New York NY 10285, Stati Uniti	Filiale	Società di merchant acquisition/servizi d'affari	Importatore di dati / Esportatore di dati	867929
American Express International (Taiwan), Inc.	Taiwan	12th Floor No. 363, Fu- Hsing North Rd., Taipei, 105, Taiwan	Controllata di maggioranza o al 100%	Emissione di carte di credito e carte di credito a saldo	Importatore di dati / Esportatore di dati	11825058
American Express International , Inc.	Stati Uniti	200 Vesey Street, New York NY 10285, Stati Uniti	Controllata di maggioranza o al 100%	Società di servizi d'affari	Importatore di dati / Esportatore di dati	13-6115802
American Express International, Inc. - Filiale - Australia	Australia	200 Vesey Street, New York NY 10285, Stati Uniti	Filiale	Società di elaborazione dati	Importatore di dati / Esportatore di dati	ABN 15000618208
American Express International, Inc. -	Germania	200 Vesey Street, New York NY	Filiale	Servizi nel settore del turismo e dei viaggi	Esportatore di dati	11988

Filiale - Germania		10285, Stati Uniti				
American Express International, Inc. - Filiale - Hong Kong	Hong Kong	200 Vesey Street, New York NY 10285, Stati Uniti	Filiale	Emissione di carte di credito e carte di credito a saldo	Importatore di dati / Esportatore di dati	BRN - 02099825
American Express International, Inc. - Filiale - Giappone	Giappone	200 Vesey Street, New York NY 10285, Stati Uniti	Filiale	Carte di credito, carte di credito a saldo, gift card e merchant acquisition	Importatore di dati / Esportatore di dati	3841
American Express International, Inc. - Filiale - Filippine	Filippine	200 Vesey Street, New York NY 10285, Stati Uniti	Filiale	Servizi di outsourcing dei processi aziendali - Servizi al cliente	Importatore di dati / Esportatore di dati	F-552
American Express International, Inc. - Filiale - Singapore	Singapore	200 Vesey Street, New York NY 10285, Stati Uniti	Filiale	Emissione di carte di credito e carte di credito a saldo e servizi finanziari correlati	Importatore di dati / Esportatore di dati	S68FC1878J
American Express International, Inc. - Filiale - Svizzera	Svizzera	200 Vesey Street, New York NY 10285, Stati Uniti	Filiale	Servizi alle affiliate AXP	Importatore di dati / Esportatore di dati	CH-020.9.900.052-2
American Express Italia S.r.l.	Italia	Viale Alexandre, Gustave Eiffel 15, 00148, Roma, Italia	Controllata di maggioranza o al 100%	Emissione di carte	Esportatore di dati	RM - 1521502
American Express Japan Co., Ltd.	Giappone	4-1-1 Toranomon, Minato- ku, Tokyo, 105-6920,	Controllata di maggioranza o al 100%	Società di servizi al cliente	Importatore di dati / Esportatore	242951

		Giappone			e di dati	
American Express Limited	Stati Uniti	200 Vesey Street, New York NY 10285, Stati Uniti	Controllata di maggioranza o al 100%	Società di network licensing	Importatore di dati / Esportatore di dati	13-2586873
American Express Marketing & Development Corp.	Stati Uniti	200 Vesey Street, New York NY 10285, Stati Uniti	Controllata di maggioranza o al 100%	Fornisce servizi di supporto per altre società Amex	Importatore di dati / Esportatore di dati	20-3083109
American Express Overseas Credit Corporation Limited	Jersey	1st Floor, Le Gallais Building, 54 Bath Street, St. Helier, JE2 4SU, Jersey	Controllata di maggioranza o al 100%	Società di finanziamento dei crediti per i titolari di carte di credito	Importatore di dati / Esportatore di dati	23072
American Express Payment Services Limited	Regno Unito	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, Regno Unito	Controllata di maggioranza o al 100%	Società di servizi d'affari	Importatore di dati / Esportatore di dati	6301718
American Express Payment Services Limited - Filiale - Germania	Germania	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, Regno Unito	Filiale	Società non operativa che detiene passività nei confronti di pensionati ed ex dipendenti che non possono essere trasferite con facilità.	Esportatore di dati	B 85745
American Express Payments Europe, S.L.	Spagna	Avda. Partenón 12-14, 28042, Madrid, Spagna	Controllata di maggioranza o al 100%	Società di merchant acquisition e servizi d'affari	Esportatore di dati	Non disponibile

American Express Payments Europe, S.L. - Filiale - Francia	Francia	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Società di merchant acquisition e servizi d'affari	Esportatore di dati	839 240 520
American Express Payments Europe, S.L. - Filiale - Germania	Germania	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Società di merchant acquisition e servizi d'affari	Esportatore di dati	HRB 112344
American Express Payments Europe, S.L. - Filiale - Italia	Italia	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Società di merchant acquisition e servizi d'affari	Esportatore di dati	14778691007
American Express Payments Europe, S.L. - Filiale - Paesi Bassi	Paesi Bassi	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Società di merchant acquisition e servizi d'affari	Esportatore di dati	39929841
American Express Payments Europe, S.L. - Filiale - Svezia	Svezia	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Società di merchant acquisition e servizi d'affari	Esportatore di dati	516411-3598
American Express Payments Europe, S.L.U. - Filiale - Austria	Austria	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Società di merchant acquisition e servizi d'affari	Esportatore di dati	FN 493466 k
American Express Payments Europe, S.L.U. - Filiale - Belgio	Belgio	Avda. Partenón 12-14, 28042, Madrid, Spagna	Filiale	Società di merchant acquisition e servizi d'affari	Esportatore di dati	0776.651.878
American Express Prepaid Card Management Corporation	Stati Uniti	18850 N, 56th St, Phoenix Arizona 85054, Stati Uniti	Controllata di maggioranza o al 100%	Emissione di carte	Importatore di dati / Esportatore di dati	30-0524568

American Express Services Europe Limited	Regno Unito	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, Regno Unito	Controllata di maggioranza o al 100%	Emissione di carte di credito e carte di credito a saldo	Importatore di dati / Esportatore di dati	1833139
American Express Services Europe Limited - Filiale - Germania	Germania	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, Regno Unito	Filiale	Emissione di carte	Esportatore di dati	57783
American Express Services Europe Limited - Filiale - Italia	Italia	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, Regno Unito	Filiale	Holding finanziaria	Esportatore di dati	5090991000
American Express Services India Private Limited	India	MGF Metropolitan - Saket, 7th Floor, Office Block, District Centre Saket, New Delhi, 110017, India	Controllata di maggioranza o al 100%	Società di servizi per le affiliate	Importatore di dati / Esportatore di dati	U65921DL1999FTC101368
American Express TLS HK Limited	Hong Kong	Suites 1701-3 and 1712-14, 17/F, 12 Taikoo Wan Road, Taikoo Shing, Hong Kong, Hong Kong	Controllata di maggioranza o al 100%	Servizi connessi ai viaggi	Importatore di dati / Esportatore di dati	62391986

American Express Travel Related Services Company, Inc.	Stati Uniti	200 Vesey Street, New York NY 10285, Stati Uniti	Controllata di maggioranza o al 100%	Merchant acquisition (ricavi da sconti)	Importatore di dati / Esportatore di dati	13-3133497
American Express, spol. s r.o.	Repubblica Ceca	Perlova 371/5, Prague 1, 110 00, Repubblica Ceca	Controllata di maggioranza o al 100%	Servizi connessi ai viaggi	Esportatore di dati	571849
Amex Agenzia Assicurativa S.r.l.	Italia	Viale Alexandre, Gustave Eiffel 15, 00148, Roma, Italia	Controllata di maggioranza o al 100%	Broker o agente assicurativo	Esportatore di dati	10190130152
Amex Asesores de Seguros, S.A. (Sociedad Unipersonal)	Spagna	Avda. Partenón 12-14, 28042, Madrid, Spagna	Controllata di maggioranza o al 100%	Broker o agente assicurativo	Esportatore di dati	A-79770608

Amex Bank of Canada	Canada	2225 Sheppard Avenue East, Suite 100, Toronto ON M2J 5C2, Canada	Controllata di maggioranza o al 100%	Banca estera diversa da una FBO (for the benefit of)	Importatore di dati / Esportatore di dati	119376804 RC0001
Amex Canada Inc.	Canada	2225 Sheppard Avenue East, Suite 100, Toronto ON M2J 5C2, Canada	Controllata di maggioranza o al 100%	Società di servizi al cliente	Importatore di dati / Esportatore di dati	1627387
Amex General Insurance Agency, Inc.	Taiwan	12th Floor No. 363, Fu-Hsing North Rd., Taipei, 105, Taiwan	Controllata di maggioranza o al 100%	Broker o agente assicurativo	Importatore di dati / Esportatore di dati	84306997
Amex Services, Inc.	Stati Uniti	200 Vesey Street, New York NY 10285, Stati Uniti	Controllata di maggioranza o al 100%	Società di servizi al cliente	Importatore di dati / Esportatore di dati	13-6115803
Centurion Finance Limited	Nuova Zelanda	Jarden House, Level 5, 21 Queen Street, Auckland, 1010, Nuova Zelanda	Controllata di maggioranza o al 100%	Servizi di cambio valuta	Importatore di dati / Esportatore di dati	104478
Centurion Finance Limited - Filiale - Australia	Australia	Jarden House, Level 5, 21 Queen Street, Auckland, 1010, Nuova Zelanda	Filiale	Servizi di cambio valuta / pagamenti internazionali	Importatore di dati / Esportatore di dati	Non disponibile

PT American Express Indonesia	Indonesia	The Plaza Complex Gondangdia, Lt 28 unit D, Jl. MH. Thamrin No.28 – 30, Menteng, Jakarta Pusat, 10350, Indonesia	Controllata di maggioranza o al 100%	Emissione di carte di credito e servizi di supporto alle carte di credito	Importatore di dati / Esportatore di dati	AHU-53498.AH.01.01.Tahun 2010
-------------------------------	-----------	--	--------------------------------------	---	---	-------------------------------

## GLOSSARIO

"AEESA" - indica American Express Europe, S.A., con sede in Avenida Partenón 12 -14, Madrid, 28042.

"Società del gruppo American Express vincolata alle BCR" o "American Express" o "la Società" - indica le Società del gruppo American Express vincolate alle Binding Corporate Rules (BCR - Norme vincolanti d'impresa), come indicato nell'Appendice [2].

"American Express Company" - indica American Express Company, con sede presso il World Financial Center, 200 Vesey St., New York, NY 10285 Stati Uniti.

"Informativa sulla Privacy di American Express" - indica l'Informativa sulla Privacy dei Titolari di Carta (per i Titolari di Carta), l'Informativa sulla Privacy per le aziende (per i Clienti aziendali), l'Informativa sulla Privacy online (per i Clienti e gli utenti che visitano il sito web), l'Informativa sulla Privacy per le assunzioni online (per i potenziali Dipendenti), o l'Informativa sulla Privacy dei dipendenti (per gli attuali Dipendenti), e altri avvisi, termini e condizioni (ad esempio per gli esercenti), comprese eventuali modifiche successive, applicabili al rapporto che intercorre tra l'Interessato e American Express.

"Normativa applicabile in materia di protezione dei dati" - indica il GDPR (e le normative nazionali di attuazione), la Direttiva e-Privacy 2002/58/CE (e le normative nazionali di attuazione) e qualsiasi altra legge e regolamento sulla protezione dei dati applicabile nello SEE (compresa eventuali modifiche successive).

"Consenso" - indica qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati personali che lo riguardano siano oggetto di Trattamento.

"Violazione dei dati" o "Violazione dei dati personali" - indica una violazione di sicurezza che comporta 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.

"Titolare del trattamento" - indica 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 dei Dati personali.

"Esportatore di Dati" - indica la Società del gruppo American Express vincolata alle BCR che trasferisce i Dati personali ai sensi delle presenti BCR.

"Importatore di dati" - indica la Società del gruppo American Express vincolata alle BCR situata al di fuori dello SEE che riceve i Dati personali (direttamente o indirettamente) dall'Esportatore di dati.

"Valutazione d'impatto sulla protezione dei dati" - indica una valutazione dell'impatto di un'attività di Trattamento pianificata sulla protezione dei Dati personali in situazioni in cui il Trattamento presenta un potenziale rischio elevato per i diritti e le libertà degli Interessati.

"Interessato/i" - indica una persona fisica identificata o identificabile che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale, per la quale il Trattamento dei Dati personali è soggetto alla Normativa applicabile in materia di protezione dei dati e trasferito nell'ambito delle presenti BCR da una Società del gruppo American Express vincolata alle BCR.

"Responsabile del trattamento" - indica la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati personali per conto e secondo le istruzioni del Titolare del trattamento.

"SEE" - indica lo Spazio Economico Europeo, che comprende tutti i paesi dell'Unione Europea nonché Islanda, Liechtenstein e Norvegia.

"GDPR" - indica il Regolamento generale sulla protezione dei dati 2016/679.

"Accordo infragruppo" - indica l'accordo infragruppo che vincola le Società del gruppo American Express vincolate alle BCR.

"Dati personali" - indica qualsiasi informazione relativa a un Interessato.

"Trattamento" o "trattare" - 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.

"Profilazione" - indica 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" - indica 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 intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

"Autorità di controllo" o "Autorità di controllo competente" - indica un'autorità pubblica indipendente relativa a un Esportatore di dati con sede nello SEE responsabile di monitorare l'applicazione della Normativa applicabile in materia di protezione dei dati.

"Paese Terzo" - indica un paese al di fuori dello SEE in cui ha sede la relativa Società del gruppo American Express vincolate alle BCR.

"Trasferimento"- indica qualsiasi trasferimento di Dati personali da una società situata nello SEE, o comunque soggetta al GDPR, a un'altra o trasferimenti successivi che sarebbero altrimenti limitati dal GDPR. Un trasferimento avviene tramite qualsiasi comunicazione, copia o divulgazione di Dati personali attraverso una rete, compreso l'accesso remoto a un database o il trasferimento da qualsiasi supporto a un altro.

AXP Interno