BINDING CORPORATE RULES
DEL GRUPPO AXA

Premessa

Il Gruppo AXA si impegna a mantenere la riservatezza dei dati ottenuti nel corso della sua attività e a rispettare tutte le leggi e i regolamenti applicabili in relazione al trattamento di Dati personali e di Categorie speciali di Dati.

Il Gruppo AXA ha una Organizzazione/Governance globale per la protezione dei dati con (i) un modello di governance per la protezione dei dati approvato dal Management Committee, (ii) un Group Data Privacy Officer, (iii) un Group Data Privacy Steering Committee, (iv) una rete mondiale di Data Privacy Officer coordinata dal Group Data Privacy Officer e (v) uno Standard sulla Riservatezza dei dati del Gruppo.

Il Gruppo AXA ha deciso di adottare una serie di Binding Corporate Rules ("BCR", Regole aziendali vincolanti) al fine di istituire adeguate tutele per garantire che i Dati personali siano protetti quando vengono trasferiti all'interno del Gruppo AXA e/o da una Società AXA o da una società impegnata in un'attività economica congiunta con Società AXA con sede in una Giurisdizione regolamentata (definita nel successivo Articolo I) a una Società AXA o a una società impegnata in un'attività economica congiunta con Società AXA con sede in altra giurisdizione in cui il trasferimento non sia altrimenti permesso dalla legge applicabile, e in caso di qualsiasi successivo trasferimento di tali dati che non sia altrimenti consentito dalla legge applicabile.

ARTICOLO I - DEFINIZIONI

Nell'uso fatto nelle BCR, nelle appendici e nell'Intragroup Agreement ("IGA" – Contratto Intra Gruppo), i seguenti termini ed espressioni, scritti con la lettera maiuscola, avranno il significato riportato di seguito:

L'"**AXA BCR Steering Committee"** è un comitato appositamente dedicato alle BCR, composto da esponenti dell'alta dirigenza del Gruppo AXA e dai Data Privacy Officer di selezionate Società AXA impattate dalle BCR.

Per **"Società AXA"** si intendono AXA, Société Anonyme con Consiglio di Amministrazione e sede legale in avenue Matignon, 25, 75008 Parigi, iscritta nel Registro del Commercio di Parigi con il numero 572 093 920; e (i) qualsiasi altra società controllata da, o che controlli AXA; si considera che una società ha il controllo di un'altra: (a) quando detiene direttamente o indirettamente una parte del capitale che le conferisce la maggioranza dei diritti di voto nelle assemblee generali dei soci di tale società; (b) quando detiene da sola la maggioranza dei diritti di voti di tale società in virtù di un contratto stipulato con altri soci o azionisti, che non sia contrario agli interessi della società; (c) quando determina de facto, mediante i diritti di voto che detiene, le decisioni alle assemblee generali dei soci di tale società; (d) in ogni caso, qualora detenga, direttamente o indirettamente, una parte dei diritti di voto superiore al 40% e qualora nessun altro socio o azionista detenga direttamente o indirettamente una percentuale superiore alla sua; (e) qualora abbia il potere di dirigere o determinare la direzione e la gestione (sia attraverso la proprietà di azioni con diritto di voto, per contratto o altro) di tale società (ii) qualsiasi gruppo di interesse economico in cui AXA e/o una o più Società del Gruppo AXA partecipa ad almeno il 50% dei costi operativi; (iii) nei casi in cui la

legge applicabile a una società limiti i diritti di voto o il controllo (così come definito in precedenza), tale società sarà ritenuta essere una società del Gruppo AXA, se i diritti di voto nelle assemblee generali dei soci o il controllo da parte di tale società del Gruppo AXA raggiunge l'importo massimo stabilito dalla suddetta legge applicabile; e (iv) tutte le Società AXA costituiscono il "Gruppo AXA".

"**Dipendenti AXA**" sono tutti i dipendenti delle Società AXA ivi compresi amministratori, tirocinanti, apprendisti e persone con status assimilato.

Per **"Gruppo AXA"** si intendono collettivamente AXA SA e tutte le Società AXA.

Per **"Società AXA impattate dalle BCR"** o "**Società AXA impattata dalle BCR**" si intendono (i) tutte le Società AXA che hanno sottoscritto l'Intra-Group Agreement in qualità di Esportatori di dati o Importatori di dati e (ii) le imprese impegnate in un'attività economica congiunta con le Società AXA e che hanno firmato il Contratto intragruppo in qualità di Esportatori di dati o di Importatori di dati.

Per **"Dipendenti delle Società BCR"** sono tutti i dipendenti delle società impegnate in un'attività economica congiunta con le Società AXA che hanno firmato il Contratto intragruppo in qualità di Esportatori di dati o di Importatori di dati.

Per **"AXA BCR Hubs"** si intendono le principali Società AXA trasversali e/o locali o altre organizzazioni AXA che partecipino all'implementazione delle BCR in collaborazione con il GDPO al fine di proteggere i Dati personali all'interno del Gruppo AXA e per il trasferimento di tali Dati personali da stati membri dello Spazio Economico Europeo ("SEE") all'interno e all'esterno del SEE.

Per **"Binding Corporate Rules"** o **"BCR"** si intendono le presenti Regole aziendali vincolanti convenute tra AXA SA e tutte le altre Società AXA impattate dalle BCR.

Per **"Titolare"** si intende una Società AXA impattata dalle BCR che, da sola o insieme ad altre, stabilisca la/e finalità, le condizioni e i mezzi di Trattamento dei Dati personali.

Per **"Violazione di Dati"** si intende una violazione della sicurezza che comporta, accidentalmente o illegalmente, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai Dati personali trasmessi, memorizzati o comunque elaborati.

Per **"Esportatore di dati"** si intende qualsiasi Titolare situato in una Giurisdizione regolamentata o Responsabile situato in una Giurisdizione regolamentata che tratti Dati personali per conto di un Titolare che trasferisca Dati personali al di fuori della Giurisdizione regolamentata in cui si trova (attraverso un Responsabile o un Responsabile terzo o meno) e abbia firmato l'Intra-Group Agreement.

Per **"Importatore di dati"** si intende qualsiasi Titolare o Responsabile che tratti Dati personali per conto di un Titolare che riceva Dati personali dall'Esportatore di dati in virtù di un Trasferimento pertinente o Successivo Trasferimento e che abbia sottoscritto l'Intra Group Agreement.

Per **"Data Privacy Officer"** o **"DPO"** si intende la persona che, in tutte le Società AXA, è responsabile di coordinarsi con il GDPO e garantire la conformità delle Società AXA alle BCR e ai requisiti applicabili in base alle leggi e ai regolamenti locali.

Per **"Soggetto interessato"** si intende qualsiasi persona fisica, che possa essere identificata, direttamente o indirettamente, mediante mezzi ragionevolmente utilizzati da qualsiasi persona fisica o giuridica, in particolare facendo riferimento a un identificativo come il nome, numero identificativo, coordinate relative a una località, identificativo online o ad uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona.

Per "**Comitato Europeo della Protezione dei Dati**" si intende l'organismo dell'Unione composto dal responsabile di un'autorità di supervisione di ogni Stato membro e dal Garante europeo della Protezione dei Dati.

Per **"SEE"** o **"Spazio Economico Europeo"** si intende lo Spazio Economico Europeo che riunisce i paesi dell'Unione Europea e i paesi membri dell'EFTA (Associazione Europea di libero scambio). Al 2 maggio 2019, il SEE comprende Austria, Belgio, Bulgaria, Cipro, Croazia, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Islanda, Irlanda, Italia, Lettonia, Liechtenstein, Lituania, Lussemburgo, Malta, Olanda, Norvegia, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna, Svezia e Regno Unito.

Per **"Esportatore Dati del SEE"** si intende qualsiasi Titolare o un Responsabile situato nel SEE che tratti Dati personali per conto di un Titolare che trasferisca Dati personali al di fuori del SEE (attraverso un Responsabile o un Responsabile terzo o meno) e abbia firmato l'Intra Group Agreement.

Per **"Soggetto interessato del SEE"** si intende qualsiasi Soggetto interessato che risultava residente in uno stato membro del SEE all'epoca in cui sono stati acquisiti i suoi Dati personali.

Le **"Clausole modello UE"** sono le clausole contrattuali standard emesse dalla Commissione Europea che offrono le sufficienti tutele richieste dal Regolamento europeo per il trasferimento di Dati personali a paesi terzi che, secondo la Commissione Europea, non garantiscono un adeguato livello di protezione dei dati.

Per **"Regolamento europeo"** si intendono le regole e le normative attuali e future relative alla protezione dei dati applicabili nei paesi del SEE.

Per **"Group Data Privacy Officer"** o **"GDPO"** si intende la persona preposta alla supervisione delle presenti Binding Corporate Rules attraverso una rete di Data Privacy Officer.

Per **"Intragroup Agreement" (Contratto intragruppo)** o **"IGA"** si intende il Contratto BCR allegato nell'Appendice 1 e qualsiasi Contratto di accettazione delle BCR (di cui all'Allegato 2 dell'Appendice 1) delle Binding Corporate Rules del Gruppo AXA, che le Società AXA impattate dalle BCR hanno firmato o devono firmare.

Per **"Trasferimento Successivo"** si intende il successivo trasferimento di Dati personali esportati in precedenza in virtù di un Trasferimento pertinente o di un trasferimento nel Sistema di Approdo sicuro USA (US Safe Harbor Scheme), a seconda dei casi:

(i) ad altra Società AXA impattata dalle BCR che si trovi in un Territorio che (se non per l'applicazione delle BCR) non offre un adeguato livello di protezione, come richiesto dalla legge sulla privacy della relativa Giurisdizione regolamentata alla base dell'originario Trasferimento pertinente; e

(ii) che non sia soggetto ad alcuna delle deroghe consentite o condizioni contemplate dalla legge sulla privacy nella relativa Giurisdizione regolamentata (che può comprendere il consenso del Soggetto interessato, tutele contrattuali esistenti,

adesione al Sistema di Approdo sicuro USA e/o sede in una giurisdizione approvata dalla Commissione Europea ai sensi del Regolamento europeo).

Per **"Dati personali"** si intende qualsiasi dato relativo a un individuo (persona fisica) che sia o possa essere identificato attraverso tali dati o attraverso i dati unitamente ad altre informazioni.

Per **"Trattamento"** si intende qualsiasi operazione o serie di operazioni effettuata ai Dati personali o a serie di Dati personali, sia con mezzi automatici o meno, quali acquisizione, registrazione, organizzazione, strutturazione, archiviazione, adattamento o modifica, reperimento, consultazione, utilizzo, separazione, incrocio, fusione, modifica, fornitura, utilizzo, divulgazione, distribuzione, divulgazione mediante trasmissione, diffusione o rendendo disponibili in altro modo, allineamento o combinazione, restrizione, cancellazione o distruzione.

Per "**Responsabile**" si intende una Società AXA impattata dalle BCR che tratti Dati personali per conto di un Titolare.

Per "**Giurisdizione regolamentata**" o "Giurisdizioni regolamentate" si intende qualsiasi giurisdizione nello SEE ed in Andorra, Svizzera, Isole Faeroe, Guernsey, Isola di Man e Jersey.

Per **"Soggetto interessato di una Giurisdizione regolamentata"** o **"Soggetti interessati di una Giurisdizione regolamentata"** si intende qualsiasi Soggetto interessato che risultava residente in una Giurisdizione regolamentata all'epoca in cui sono stati acquisiti i suoi Dati personali.

Per "**Trasferimento pertinente**" si intende il trasferimento di Dati personali (nella misura in cui tali Dati personali non siano stati oggetto in precedenza di un Trasferimento pertinente o Trasferimento Successivo):

(i) da una Società AXA impattata dalle BCR che sia un Esportatore di Dati ad altra Società AXA impattata dalle BCR che si trovi in un territorio che (se non per l'applicazione delle BCR) non offre un adeguato livello di protezione, come richiesto dalla legge sulla privacy della relativa Giurisdizione regolamentata dell'Esportatore di Dati; e

(ii) che non sia soggetto ad alcuna delle deroghe o condizioni consentite contemplate dalla legge sulla privacy nella relativa Giurisdizione regolamentata (che può comprendere il consenso del Soggetto interessato, tutele contrattuali esistenti, adesione al Sistema di Approdo sicuro USA e/o sede in una giurisdizione approvata dalla Commissione Europea ai sensi del Regolamento europeo).

Per **"Categorie speciali di Dati"** si intendono i dati contemplati dall'Articolo IV sezione 2.

Per "**Autorità di vigilanza**" o "**Data Protection Authority"** o **"DPA"** si intende l'autorità amministrativa ufficialmente preposta alla protezione dei Dati personali in ogni Giurisdizione regolamentata in cui è presente il Gruppo AXA (per esempio in Francia questa autorità è la *Commission Nationale de l'Informatique et des Libertés*; in Spagna è l'*Agencia Espanola de Proteccion de Datos,*etc.). Per evitare qualsiasi dubbio, il termine "Autorità di vigilanza" comprende qualsiasi sostituto o successore di un'Autorità per la protezione dei dati.

Per **"Terza parte"** si intende qualsiasi persona fisica o giuridica (ivi comprese le Società AXA/Società AXA impattate dalle BCR), autorità pubblica, agenzia o qualsiasi altro organismo diverso dal Soggetto interessato, dal Titolare, dal Responsabile e dalle persone che, sotto la diretta autorità del Titolare o del Responsabile, siano autorizzate a trattare i Dati personali del Soggetto interessato.

ARTICOLO II - SCOPO

Lo scopo delle BCR è garantire un adeguato livello di protezione dei Dati personali nell'ambito di un Trasferimento pertinente o Trasferimento Successivo da una Società AXA o da una società impegnata in un'attività economica congiunta con Società AXA con sede in una Giurisdizione regolamentata a una Società AXA o a una società impegnata in un'attività economica congiunta con Società AXA con sede in altra giurisdizione.

ARTICOLO III - AMBITO DI APPLICAZIONE

1. Ambito di applicazione geografico

Il Gruppo AXA è presente in più di 50 paesi e oltre 150 000 Dipendenti AXA e distributori di AXA sono impegnati a servire milioni di clienti.

Le presenti BCR si applicano esclusivamente ai Trasferimenti pertinenti da Esportatori di Dati con sede in una Giurisdizione regolamentata a Importatori di Dati con sede in altra giurisdizione e Trasferimenti rilevanti dagli Importatori di dati situati in un'altra giurisdizione a un Esportatore di dati in una giurisdizione regolamentata che segue questo trasferimento pertinente iniziale, nonché ai Trasferimenti successivi, e il ricorso contro violazioni ai sensi delle disposizioni relative a Diritti a beneficio di terze parti, Reclami e Responsabilità delle presenti BCR (contemplati dagli Articoli VII, VIII e IX delle stesse) sono limitati ai Soggetti interessati delle Giurisdizioni regolamentate.

Sebbene le Società AXA impattate dalle BCR possano avere ovunque processi necessari per le BCR implementate, le Società AXA impattate dalle BCR non forniscono garanzie conformi alle BCR per i Dati personali che non siano soggetti a una legge sulla privacy in una Giurisdizione regolamentata, ossia che non vengano trasferiti da una Giurisdizione regolamentata, per es.:

- se una Società AXA con sede negli USA trasferisce i suoi Dati personali a una Società AXA con sede in India, tale trasferimento e il relativo trattamento non saranno soggetti alle BCR; o

- se una Società AXA con sede in Giappone trasferisce i suoi Dati personali a una Società AXA con sede a Singapore, tale trasferimento e il relativo trattamento non saranno soggetti alle BCR.

2. Ambito di applicazione materiale

a. Ambito delle Società AXA impattate dalle BCR e applicabilità nei confronti dei Dipendenti AXA

Le presenti BCR vincolano tutte le Società AXA e società impegnate in un'attività economica congiunta con Società AXA che hanno firmato un Intra-Group Agreement in cui indicano ed esprimono l'accettazione delle BCR elencate nell'Allegato 1 all'Appendice 1 o che hanno accesso all'Intra-Group Agreement. Ogni Società AXA o società impegnata in un'attività economica congiunta con Società AXA che firmi un IGA diventa una Società AXA impattata dalle BCR a partire dalla data della firma o (se successiva) da qualsiasi Data di decorrenza indicata nell'IGA applicabile.

Conformemente alla legge applicabile in tema di lavoro, le presenti BCR sono vincolanti per e applicabili ai Dipendenti AXA e ai Dipendenti delle Società BCR di tutte le Società AXA impattate dalle BCR attraverso qualsivoglia delle seguenti disposizioni, in ogni Società AXA impattata dalle BCR:

- il rispetto delle politiche interne AXA vincolanti, o
- il rispetto di un contratto collettivo vincolante, o
- il rispetto di una clausola del contratto di assunzione, o
- qualsiasi altro mezzo idoneo a rendere le BCR vincolanti per i Dipendenti AXA o per i Dipendenti delle Società BCR nel rispettivo paese.

Conformemente alla legge sul lavoro applicabile, alle regole interne e ai contratti di assunzione, ogni Società AXA impattata dalle BCR può adottare provvedimenti disciplinari nei confronti dei suoi Dipendenti AXA o Dipendenti delle Società BCR, in particolare in caso di:

- violazione delle presenti BCR da parte di un Dipendente AXA o Dipendenti delle Società BCR,
- mancata applicazione delle raccomandazioni e dei consigli emessi dai Data Privacy Officer (i "DPO") in seguito a una verifica di conformità,
- mancata cooperazione nella verifica della conformità alle BCR effettuata dai DPO, o con le autorità pertinenti responsabili della protezione dei Dati personali.

b. Ambito dei Dati personali e delle attività di trattamento

La/e finalità dei trasferimenti di Dati personali e del Trattamento effettuato dopo i trasferimenti è/sono supportare e favorire le attività commerciali di AXA.

Le aree di competenza di AXA si rispecchiano in una gamma di prodotti e servizi adattati alle esigenze di ogni cliente in tre principali linee di business: assicurazione danni, vita & risparmio, e asset management:

- il ramo danni comprende l'assicurazione di beni e responsabilità. Copre una vasta gamma di prodotti e servizi destinati ai nostri clienti privati o aziendali, ivi compresi i servizi di assistenza e l'assicurazione internazionale per le grandi aziende, come per esempio Marine e Aviation;
- il nostro segmento assicurazione vita individuale e collettivo comprende prodotti di risparmio e pensione, da un lato, e dall'altro prodotti per la salute e la protezione personale. I prodotti per risparmio e pensione soddisfano l'esigenza di mettere da parte un capitale per finanziare un'attività futura, un progetto speciale o la pensione. La protezione personale copre i rischi correlati all'integrità fisica, alla salute o alla vita di un individuo. AXA offre anche ai clienti privati in alcuni paesi un semplice ventaglio di servizi e prodotti bancari che integrano l'offerta assicurativa;
- la divisione asset management si occupa dell'investimento e della gestione di beni per le società assicurative del Gruppo e per i loro clienti, nonché per terze parti, clienti privati e istituzionali.

Il supporto alle attività operative di AXA comprende:

- capacità di previsione (definire la visione aziendale a lungo termine, sviluppare la strategia di business, gestire un'iniziativa strategica, controllare i progressi);
- progettazione (sviluppare la strategia del prodotto, definire la politica di rischio, progettare, sviluppare & lanciare un prodotto, mantenere un portafoglio di prodotti esistente);
- distribuzione (sviluppare una strategia di distribuzione, gestire e controllare le reti di distribuzione, svolgere attività di marketing, gestire il rapporto con il cliente, personalizzare l'offerta, vendere, premiare le buone prestazioni di vendita);
- produzione (sottoscrivere, amministrare una polizza, riscuotere premi, monitorare il portafoglio di polizze);
- assistenza (gestire una catastrofe, gestire un reclamo, prestare servizi al cliente, gestire gli ausiliari, rilevare frodi, gestire la surrogazione e recuperare fondi per le richieste di indennizzo dalla riassicurazione, gestire il salvataggio di relitti, controllare la gestione dei sinistri);

- gestione delle finanze (pianificare e controllare le finanze, gestire gli investimenti, gestire le finanze aziendali, approvare le attività, gestire i beni in conto capitale, analizzare la finanza, gestire la liquidità, gestire le attività di tesoreria e cassa, gestire le imposte, rispettare i regolamenti, gestire la riassicurazione);
- gestione dell'information technology (gestire il rapporto IT con il cliente, offrire e provvedere alla manutenzione di soluzioni, offrire & supportare servizi IT, gestire l'infrastruttura IT, gestire l'organizzazione IT, gestire la sicurezza IT);
- sviluppo & gestione risorse umane (amministrare le risorse umane, gestire le risorse umane, provvedere alla comunicazione con le risorse umane, gestire le parti sociali e i comitati aziendali);
- gestione degli acquisti (gestire i fornitori e i contratti, acquistare, ricevere merci e servizi, gestire le fatture fornitori, approvare e convalidare i pagamenti, effettuare reporting sugli acquisti e analisi della performance);
- gestione del rischio (gestire il rischio finanziario, gestire il rischio dell'investimento, gestire il rischio operativo, effettuare proiezioni, calcolare la redditività in rapporto al rischio),
- altre funzioni di supporto (occuparsi delle comunicazioni esterne, supporto giuridico, gestire il miglioramento e cambiamento, auditing interno, funzioni centralizzate).

Tutte le tipologie e categorie di Dati personali trattati dalle Società AXA impattate dalle BCR nello svolgimento della propria attività devono rientrare nell'ambito delle presenti BCR. Tali tipologie e categorie comprendono: i Dati personali acquisiti da clienti, potenziali clienti, sinistrati, Dipendenti AXA o Dipendenti delle Società BCR, candidati a posti di lavoro, agenti, fornitori e altre terze parti.

Le categorie di Dati personali trattati dalle Società AXA impattate dalle BCR che sono tenute o sono in grado di acquisirli localmente conformemente alla legislazione applicabile comprendono:

- stato civile/identità/dati utili per l'identificazione,
- vita professionale,
- vita personale,
- dati relativi alle connessioni,
- coordinate relative a una località,
- numero di previdenza sociale,
- informazioni di carattere economico e finanziario,
- reati, sentenze di condanna, misure di sicurezza,
- dati sulle convinzioni filosofiche, politiche, religiose, riguardanti l'adesione a sindacati, la vita sessuale, le condizioni di salute, l'origine razziale,
- dati biometrici,
- dati riguardanti la genetica,
- morte di persone,
- valutazione delle difficoltà sociali delle persone,
- dati sull'assicurazione sanitaria.

Le BCR coprono le tipologie di trattamento automatico e manuale.

ARTICOLO IV - PRINCIPI DI TRATTAMENTO

Per qualsiasi Trattamento di Dati personali che rientri nell'ambito definito nell'ARTICOLO III – AMBITO DI APPPLICAZIONE, saranno rispettati i Principi di trattamento indicati di seguito.

1. Principi generali

Ciascuna delle Società AXA impattate dalle BCR garantisce e conviene di ottemperare agli obblighi previsti dalla Legge applicabile e dall'Autorità per la protezione dei dati locale competente per il Trattamento originario di Dati personali, che vengano successivamente trasferiti nell'ambito di un Trasferimento pertinente o Trasferimento Successivo ai sensi delle BCR.

Ciascuna delle Società AXA impattate dalle BCR accetta che il Trattamento dei Dati personali effettuato sotto il proprio controllo, ivi compresi i trasferimenti di dati, continuerà a essere effettuato conformemente alle disposizioni delle presenti BCR e in particolare ai seguenti principi minimi generali di protezione dei dati:

- i Dati personali devono essere ottenuti in modo lecito, corretto e trasparente e con il diritto di informazione dell'Interessato, salvo qualora tale informazione non sia necessaria per via di eccezioni legali; essi devono essere trattati soltanto se il Soggetto interessato ha espresso il proprio consenso o se il Trattamento è altrimenti permesso dalle leggi applicabili.

- I Dati personali devono essere acquisiti soltanto per scopo/i specificato/i, esplicito/i e legittimo/i e non devono essere ulteriormente trattati in alcun modo incompatibile con tale/i scopo/i. I Dati personali saranno resi disponibili soltanto a terze parti per questo/i scopo/i o nelle modalità altrimenti consentite dalle leggi applicabili.

- Devono essere implementati appropriati controlli e procedure tecniche ed organizzative per garantire la sicurezza dei Dati personali e impedirne l'accesso o la divulgazione non autorizzata, il potenziale danno che potrebbe derivare da alterazione, distruzione accidentale o illecita o perdita accidentale di dati, e contro tutte le altre forme illecite di Trattamento. Tenendo conto degli obblighi di legge, delle best practice e del costo di implementazione, devono essere messe a punto misure di sicurezza per garantire un livello di sicurezza appropriato ai rischi rappresentati dal Trattamento e dalla natura dei Dati personali da proteggere.

- Devono essere adottate misure tecniche e organizzative appropriate, sia nel momento in cui sono definiti i mezzi per il trattamento, sia nel momento del trattamento stesso, per implementare in modo efficace i principi di protezione dei dati e integrare le necessarie misure di salvaguardia previsti nel disegno nel trattamento, al fine di soddisfare i requisiti del Regolamento europeo e proteggere i diritti dei soggetti interessati.

- Devono essere implementate misure tecniche e organizzative appropriate per garantire che, per impostazione predefinita, siano trattati soltanto i Dati personali necessari per ogni scopo specifico del trattamento.

- I Dati personali raccolti devono essere accurati, completi per la/e finalità prevista/e e, quando necessario, aggiornati.

- I Dati personali acquisiti devono essere minimizzati, *cioè* adeguati, pertinenti e limitati a quanto è effettivamente necessario in relazione alla/e finalità per cui vengono acquisiti e/o ulteriormente trattati.

- I Dati personali non devono essere conservati per un periodo di tempo superiore a quello necessario per la/e finalità per cui sono stati ottenuti, fatto salvo quanto altrimenti previsto dalle leggi applicabili. Maggiori informazioni sui periodi di conservazione dei dati pertinenti sono disponibili nella politica di conservazione dei dati applicabile in ogni Società AXA impattata dalle BCR.

- Devono essere implementate procedure per garantire una tempestiva risposta alle richieste di informazioni dei Soggetti interessati in modo che possano debitamente esercitare i propri diritti di accesso, rettifica, cancellazione dei propri Dati personali e i diritti di limitazione e opposizione al Trattamento (fatto salvo quanto diversamente previsto dalla Legge applicabile) e revocare il consenso laddove il Trattamento sia fondato su questa base legale.

I Dati personali devono essere trattati soltanto qualora tale Trattamento sia fondato su basi legali, ivi compreso per esempio qualora:

- il Soggetto interessato abbia espresso il proprio consenso; o
- il Trattamento sia necessario per l'esecuzione di un contratto di cui il Soggetto interessato sia parte o per adempiere ad una richiesta del Soggetto interessato prima della stipula di un contratto; o
- il Trattamento sia necessario per ottemperare a un obbligo di legge a cui il Titolare sia soggetto; o
- il Trattamento sia necessario al fine di proteggere gli interessi vitali del Soggetto interessato; o
- il Trattamento sia necessario per lo svolgimento di un compito nell'interesse pubblico o nell'esercizio dell'autorità ufficiale conferita al Titolare o a una terza parte a cui i Dati personali vengano divulgati; o
- il Trattamento sia necessario ai fini dei legittimi interessi perseguiti dal Titolare o dalla/e terza/e parte/i a cui i Dati personali vengano divulgati, tranne qualora su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali del Soggetto interessato.

Qualora il Trattamento dei Dati personali si basi esclusivamente sul trattamento automatizzato di dati, inclusa la profilazione, e produca effetti legali che riguardano o hanno notevoli conseguenze sui Soggetti interessati, gli stessi hanno il diritto di non essere soggetti a tale decisione, eccetto qualora tale Trattamento:

- sia necessario nell'ambito della stipula o esecuzione di un contratto, a condizione che la richiesta di stipula o esecuzione del contratto, presentata dal Soggetto interessato, sia stata soddisfatta o vi siano misure adeguate a tutelarne i legittimi interessi, per esempio accordi che gli consentano di esprimere il suo punto di vista e contestare la decisione; o
- sia autorizzato da una legge che stabilisce anche misure per tutelare i legittimi interessi del Soggetto interessato; o
- si basi sul consenso esplicito del Soggetto interessato,

a condizione che vi siano misure adeguate per salvaguardare i suoi interessi legittimi, quali accordi che gli consentano di ottenere un intervento umano, di esprimere il proprio punto di vista e contestare la decisione.

Ogni Titolare terrà un registro di tutte le categorie delle attività di trattamento effettuate sui Dati personali di Soggetti interessati SEE e, su richiesta, metterà il registro a disposizione dell'Autorità per la protezione dei dati coordinatrice e di qualsiasi altra Autorità pertinente per la protezione dei dati.

Ogni Titolare effettuerà Valutazioni dell'impatto sulla protezione dei dati laddove sia necessario per il trattamento di operazioni che potrebbero comportare un rischio elevato per i diritti e le libertà dei Soggetti interessati SEE. Laddove una Valutazione dell'impatto sulla protezione dei dati indichi che il trattamento comporterebbe un rischio elevato, in assenza di misure adottate dalla Società AXA impattata dalle BCR per limitare il rischio dovrebbe essere consultata l'Autorità per la protezione dei dati coordinatrice oppure qualsiasi altra Autorità per la protezione dei dati pertinente.

2. Categorie speciali di Dati personali

Ai fini delle presenti BCR, le Categorie speciali di Dati comprenderanno qualsiasi Dato personale relativo a:

- origine razziale o etnica, opinioni politiche o credo religioso o convinzioni filosofiche del Soggetto interessato;
- appartenenza del Soggetto interessato a un sindacato;
- salute fisica o mentale o condizione o vita sessuale oppure orientamento sessuale del Soggetto interessato, dati genetici, dati biometrici allo scopo unicamente di identificare una persona fisica;
- dati specifici ritenuti appartenenti a Categorie speciali di Dati in virtù della legge e del regolamento applicabile (es. informazioni mediche);
- reato o presunto reato commesso dal Soggetto interessato o condanna; o
- qualsiasi procedimento per un reato o presunto reato commesso dal Soggetto interessato, l'archiviazione di tale procedimento o la sentenza di qualsiasi tribunale in tale procedimento.

L'elenco riportato in precedenza non deve essere in alcun modo considerato esaustivo per quanto riguarda Categorie speciali di Dati, in quanto la legislazione locale può comprendere ulteriori categorie che, in tali casi e ove applicabile, saranno considerate Categorie speciali di Dati dall'Esportatore di dati e dall'Importatore di dati.

Il Trattamento delle Categorie speciali di Dati è vietato salvo qualora:

1. il Soggetto interessato abbia espresso il suo esplicito consenso al Trattamento di tali Categorie speciali di Dati e tale consenso sia considerato valido ai sensi della legge e del regolamento applicabile; o
2. il Trattamento sia necessario al fine di adempiere gli obblighi e rispettare i diritti specifici del Titolare o del Soggetto interessato nel campo della legge sul lavoro, della previdenza e della sicurezza sociale, nella misura in cui sia autorizzato dalla legge applicabile fornendo adeguate tutele; o
3. il Trattamento sia necessario per tutelare gli interessi vitali del Soggetto interessato o di qualsiasi altra persona qualora il Soggetto interessato sia fisicamente o legalmente incapace di esprimere il suo consenso; o
4. il Trattamento avvenga nel corso di legittime attività con adeguate garanzie da parte di una fondazione, associazione o altro organismo senza scopo di lucro con un fine politico, filosofico, religioso o sindacale, e a condizione che il Trattamento si riferisca esclusivamente ai membri dell'organismo o alle persone che intrattengano contatti regolari con lo stesso in relazione alla/e sua/e finalità e che i Dati personali non siano divulgate a terze parti senza il consenso dei Soggetti interessati; o
5. il Trattamento si riferisca a Categorie speciali di Dati che sono stati resi pubblici dal Soggetto interessato; o
6. il Trattamento di Categorie speciali di Dati sia necessario per l'attivazione, l'esercizio o la difesa di azioni legali; o
7. il Trattamento sia necessario per ragioni di interesse pubblico rilevante, sulla base delle leggi dell'Unione o dello Stato membro. Il Trattamento sarà commisurato allo scopo perseguito, rispetterà l'essenza del diritto alla protezione dei dati e fornirà misure adeguate e specifiche a salvaguardia dei diritti fondamentali e degli interessi del soggetto interessato; o
8. il Trattamento delle Categorie speciali di Dati sia necessario ai fini di medicina preventiva o del lavoro, per la valutazione della capacità lavorativa del dipendente, diagnosi medica, prestazione di cure o trattamenti sanitari o di carattere sociale o gestione di servizi sanitari o sistemi di assistenza sociale o sulla base della legislazione dell'Unione o dello Stato membro o conformemente a un contratto con un

professionista nel campo sanitario, soggetto alle condizioni e salvaguardie e laddove questi dati siano trattati:
    - o da un professionista soggetto all'obbligo di segreto professionale, o
    - o da altra persona soggetta a un equivalente obbligo di segretezza;
9. il Trattamento sia necessario per ragioni di pubblico interesse nel settore della sanità pubblica sulla base della legislazione dell'Unione o dello Stato membro che fornirà misure adeguate e specifiche per salvaguardare i diritti e le libertà del Soggetto interessato, in particolare il segreto professionale;
10. il Trattamento sia necessario a scopo di archiviazione nell'interesse pubblico, ai fini della ricerca scientifica o storica o per finalità statistiche, conformemente al Regolamento europeo basato sulle leggi dell'Unione o dello Stato membro. Il Trattamento sarà commisurato allo scopo perseguito, rispetterà l'essenza del diritto alla protezione dei dati e fornirà misure adeguate e specifiche per salvaguardare i diritti fondamentali e gli interessi del Soggetto interessato;
11. il Trattamento sia altrimenti consentito ai sensi della legge applicabile del paese dove ha sede l'Esportatore di dati.

3. Subappalto del trattamento

Qualora il Trattamento sia effettuato da un subappaltatore per conto di un Importatore di dati, quest'ultimo otterrà la previa autorizzazione scritta dell'Esportatore di dati, sceglierà un subappaltatore che offra sufficienti garanzie per implementare appropriate misure tecniche di sicurezza e misure organizzative per garantire che il Trattamento sia effettuato conformemente alle BCR, e l'Importatore di dati deve assicurarsi che il subappaltatore rispetti tali misure. L'Importatore di dati che sceglie il subappaltatore si assicurerà che quest'ultimo accetti le suddette misure tecniche di sicurezza e misure organizzative per iscritto sottoscrivendo un contratto in linea con il Regolamento europeo, in cui si prevede in particolare che il subappaltatore agirà unicamente in base alle istruzioni dell'Importatore di dati.

4. Trasferimenti di dati

4.1 Trasferimenti di dati all'interno del Gruppo AXA e società impegnate in un'attività economica congiunta con le Società AXA

I Dati personali non possono essere trasferiti a un Importatore di dati che abbia sede in un paese al di fuori del SEE (o in caso di esportazione da altra Giurisdizione regolamentata, al di fuori di tale Giurisdizione regolamentata), finché l'Esportatore di dati non abbia stabilito che l'Importatore di dati è vincolato:

- dalle presenti BCR, o,
- da altre misure che permettono il trasferimento di Dati personali ai sensi della legge applicabile (es., Clausole Modello UE).

Come rispecchiano i concetti di "Trasferimento pertinente" e "Trasferimento Successivo", le BCR si applicano soltanto ai trasferimenti che non sono già contemplati da altre misure che permettono i trasferimenti stessi, fatto salvo quanto altrimenti convenuto per iscritto tra l'Esportatore di dati e l'Importatore di dati.

4.2 Trasferimenti di dati al di fuori del Gruppo AXA e società impegnate in un'attività economica congiunta con le Società AXA

Per tutti i trasferimenti a una società terza al di fuori del SEE (in caso di esportazioni dal SEE, e altrimenti al di fuori della relativa Giurisdizione regolamentata) non vincolata dalle presenti BCR, ogni Importatore di dati deve impegnarsi a:

- quando trasferisce a un responsabile, firmare un contratto di trattamento con il responsabile terzo per prevedere un'adeguata tutela dei dati trattati in base agli standard europei, per esempio utilizzando le Clausole modello UE proposte dalla Commissione Europea o da qualsiasi contratto che preveda un obbligo quanto meno equivalente; o

- adottare tutte le necessarie cautele per il trasferimento di Dati personali conformemente alla legge applicabile (es. Clausole modello UE).

5. Violazione dei dati

In caso di Violazione di Dati personali di Soggetti interessati di una Giurisdizione regolamentata, le Società AXA impattate dalle BCR, interessate, comunicheranno senza indugio la Violazione di Dati al/ai DPO delle Società AXA impattate dalle BCR a loro volta interessate, ed anche al GDPO qualora siano coinvolti più di 1.000 Soggetti interessati di una Giurisdizione regolamentata.

Le Società AXA impattate dalle BCR che siano Titolari coinvolti in una Violazione di dati che potrebbe determinare un rischio elevato per i diritti e le libertà dei Soggetti interessati di una Giurisdizione regolamentata ne daranno comunicazione direttamente anche ai Soggetti interessati di una Giurisdizione regolamentata.

Qualsiasi comunicazione di una Violazione di dati sarà documentata e deve comprendere almeno:
- i fatti relativi alla Violazione dei dati,
- le probabili conseguenze della Violazione di dati,
- l'azione correttiva adottata per affrontare la Violazione di dati incluse, se appropriate, misure per limitare i suoi possibili effetti negativi.

Tale documentazione sarà resa disponibile, a richiesta, all'Autorità coordinatrice per la protezione dei dati e a qualsiasi altra Autorità pertinente per la protezione dei dati.

ARTICOLO V - DIRITTI DI INFORMAZIONE, ACCESSO, RETTIFICA, CANCELLAZIONE E BLOCCO DEI DATI

Nel caso di Trattamento di Dati personali da parte di un Importatore di dati, i Soggetti interessati di una Giurisdizione regolamentata hanno diritto, previa richiesta scritta, di:

- ottenere copia della versione per il pubblico di queste BCR dal sito internet AXA, dal sito web Intranet AXA, o dal DPO, previa richiesta ed entro un ragionevole lasso di tempo;
- richiedere informazioni sui Dati personali archiviati ad essi relativi, ivi comprese le informazioni relative alle modalità di acquisizione dei Dati personali;
- ottenere l'elenco dei destinatari o delle categorie di destinatari a cui vengono trasferiti i Dati personali;
- ottenere informazioni relative alla/e finalità dell'acquisizione dei loro Dati personali e del relativo trasferimento;
- ottenere senza indugio la rettifica dei loro Dati personali, qualora siano imprecisi;
- opporsi al Trattamento dei Dati personali sulla base di motivazioni in relazione alla loro specifica situazione, fatto salvo quanto diversamente previsto dalle leggi applicabili;
- richiedere la cancellazione senza indugio dei Dati personali se legalmente possibile e sulla base delle motivazioni specificate ai sensi del Regolamento europeo;
- ottenere la limitazione del trattamento, conformemente al Regolamento europeo,
- ottenere qualsiasi altra informazione che sia necessaria ai sensi della legge locale applicabile,

in ogni caso, fatto salvo ulteriori diritti previsti dalla legge sulla privacy della Giurisdizione regolamentata in cui il Soggetto interessato della Giurisdizione regolamentata era residente al momento in cui i suoi Dati personali sono stati acquisiti.

ARTICOLO VI - INIZIATIVE PER L'IMPLEMENTAZIONE DELLE BCR

1. Programma di formazione

Le Società AXA impattate dalle BCR si impegnano a implementare programmi di formazione sulla protezione dei Dati personali per i Dipendenti AXA o Dipendenti delle Società BCR coinvolti nel Trattamento di Dati personali e sullo sviluppo degli strumenti utilizzati per trattare i Dati personali in relazione ai principi contemplati dalle presenti BCR.

I principi generali per la formazione e la consapevolezza saranno elaborati a livello centrale, e saranno condivisi esempi pratici, mentre lo sviluppo e l'implementazione finali delle sessioni di formazione e consapevolezza (es. e-learning, in aula) saranno compito di ogni Società AXA impattata dalle BCR, in linea con le leggi e i processi applicabili.

Ogni Società AXA impattata dalle BCR stabilirà come effettuare il controllo del livello di formazione completata con successo. Ogni Società AXA impattata dalle BCR stabilirà inoltre la periodicità di aggiornamento della formazione, la formazione sulla protezione dei Dati personali di Dipendenti AXA o dei Dipendenti delle Società BCR neoassunti nell'ambito della loro sessione di insediamento quando entrano in una Società AXA impattata dalle BCR, e la formazione appositamente dedicata ai Dipendenti AXA e ai Dipendenti delle Società BCR che sono coinvolti più da vicino in aspetti critici dei Dati personali.

2. Governance BCR

Omissis

3. Responsabilità per le BCR e Programma di verifica della conformità alle BCR

Omissis

4. Accesso alle BCR e divulgazione delle BCR ai Soggetti interessati di Giurisdizioni regolamentate

Il requisito di informazione sulle BCR dei Soggetti interessati di Giurisdizioni regolamentate che non hanno accesso al sito web Intranet di AXA in qualità di clienti, individui assimilati (sinistrati, vittime di incidenti, e altri beneficiari non sottoscrittori di una polizza assicurativa), candidati a posti di lavoro e fornitori si attua pubblicando la versione per il pubblico delle BCR sul sito web pubblico di AXA.

Il requisito di informazione sulle BCR dei Soggetti interessati di Giurisdizioni regolamentate che hanno accesso al sito web dell'Intranet AXA in qualità di Dipendenti AXA e individui assimilati (es. agenti, rappresentanti) si attua pubblicando la versione per il pubblico delle BCR sul sito web Intranet di AXA.

Ulteriori modalità facoltative di informazione di clienti, fornitori, Dipendenti AXA e Dipendenti delle Società BCR presso le singole Società AXA impattate dalle BCR possono comprendere: fornitura di informazioni a clienti nell'ambito di una lettera/comunicazione su vari argomenti, fornitura di informazioni a clienti attraverso un'Agenzia – es. attraverso l'accesso degli agenti all'intranet, e fornitura di informazioni ai Dipendenti AXA e ai Dipendenti delle Società BCR attraverso comitati aziendali o altri organismi competenti di rappresentanza dei dipendenti. In molti casi, non è possibile (in quanto eccessivamente difficile e costoso) inviare una lettera dedicata a tutti i clienti, quali sinistrati, vittime di incidenti, o beneficiari di polizza che non sono assicurati o sottoscrittori di polizza.

ARTICOLO VII - DIRITTI A BENEFICIO DI TERZE PARTI

È intenzione di tutti gli Esportatori di dati concedere ai Soggetti interessati di Giurisdizioni regolamentate diritti a beneficio di terze parti ai sensi delle presenti BCR in relazione ai Trasferimenti pertinenti e Trasferimenti Successivi. Di conseguenza, ogni Esportatore di dati riconosce e conviene espressamente che i Soggetti interessati di Giurisdizioni regolamentate possono esercitare i propri diritti in relazione ai Trasferimenti pertinenti e ai Trasferimenti Successivi conformemente alle disposizioni degli Articoli IV.1, IV.2, IV.4, V, VII, VIII, IX, X, XII.3 e XIII delle presenti BCR e che l'inadempimento da parte dell'Esportatore di dati dei propri obblighi ai sensi di tali Articoli in queste circostanze potrebbe far insorgere per il Soggetto interessato della Giurisdizione regolamentata in questione il diritto di proporre azioni legali a propria tutela e, se del caso e nella misura prevista dalla legge applicabile, diritti di risarcimento (a seconda dei casi in considerazione della violazione commessa e del danno subito).

Si specifica espressamente che i diritti concessi a terze parti nelle modalità indicate in precedenza sono rigorosamente limitati ai Soggetti interessati di giurisdizioni regolamentate in relazione ai Trasferimenti pertinenti e ai Trasferimenti Successivi e non saranno in nessun caso estesi o interpretati in modo da estendersi a Interessati di giurisdizioni non regolamentate o altri trasferimenti di Dati personali.

ARTICOLO VIII - RECLAMI

Una delle responsabilità delle Società AXA impattate dalle BCR è avere un processo interno di gestione dei reclami. In caso di controversia, i Soggetti interessati di Giurisdizioni regolamentate possono presentare, conformemente alla pertinente procedura locale, un reclamo relativo a qualsiasi trattamento illecito o inappropriato dei loro Dati personali che sia in qualunque modo incompatibile con le presenti BCR, a:

- Data Privacy Officer,
- alla pertinente Autorità per la Protezione dei Dati che sarà o l'Autorità per la protezione dei dati nella Giurisdizione regolamentata del suo luogo di residenza abituale quando sono stati acquisiti i Dati personali interessati dal reclamo o il luogo dell'asserita violazione e
- alle giurisdizioni competenti di un paese SEE a scelta del Soggetto interessato: il Soggetto interessato può scegliere di agire avanti le autorità giudiziarie del paese SEE in cui l'Esportatore di dati ha una sede o avanti le autorità giudiziarie del paese SEE in cui il Soggetto interessato aveva la propria residenza abituale al momento dell'acquisizione dei Dati personali interessati dal reclamo.

A scanso di dubbio, si conviene che qualora non sia soddisfatto delle risposte del Data Privacy Officer, il Soggetto interessato di una Giurisdizione regolamentata ha il diritto di presentare un reclamo dinanzi alla pertinente Autorità per la Protezione dei Dati e/o le giurisdizioni competenti del paese conformemente al precedente paragrafo.

Ogni Società AXA impattata dalle BCR avrà sul suo sito web strumenti pratici che permettono ai Soggetti interessati di Giurisdizioni regolamentate di presentare i loro reclami, ivi compreso almeno uno di quelli elencati di seguito:

- link a un modulo di reclamo;
- indirizzo e-mail;
- numero di telefono;
- indirizzo postale.

A meno che si riveli particolarmente difficile reperire le informazioni necessarie per svolgere l'indagine, l'indagine relativa ai reclami deve essere avviata entro un (1) mese dalla data in

cui viene presentato il reclamo. In presenza di difficoltà particolari e considerata la complessità e il numero di richieste, il periodo di un (1) mese può essere esteso ad un massimo di altri due (2) mesi. In tal caso i Soggetti interessati della Giurisdizione regolamentata saranno informati di conseguenza.

ARTICOLO IX - RESPONSABILITÀ

1. Posizione generale

Ogni Società AXA impattata dalle BCR avrà la responsabilità esclusiva delle violazioni delle BCR che ricadono sotto la sua responsabilità, nei confronti di, a seconda dei casi, altre Società AXA impattate dalle BCR, le competenti Autorità per la Protezione dei dati delle Giurisdizioni regolamentate e i Soggetti interessati di Giurisdizioni regolamentate, nella misura prevista dalla legge e dal regolamento applicabili.

Nei limiti previsti dalla legge e dalla regolamentazione applicabile e ai sensi degli Articoli IX(2) e IX(3), ogni Esportatore di dati è singolarmente responsabile di qualsiasi danno che un Soggetto interessato di una Giurisdizione regolamentata possa subire a causa di qualsiasi violazione delle BCR commessa dallo stesso Esportatore di dati o da un Importatore di dati che abbia ricevuto i Dati personali trasferiti da una Giurisdizione regolamentata in virtù di un Trasferimento pertinente o Trasferimento Successivo che abbia origine dal relativo Esportatore di dati.

Nei limiti previsti dalla legge e dalla regolamentazione applicabile e ai sensi degli Articoli IX(2) e IX(3), qualora i Dati personali di un Soggetto interessato del SEE provengano da un Esportatore di dati, ogni Esportatore di dati del SEE è singolarmente responsabile di qualsiasi danno che un Soggetto interessato del SEE possa subire a causa di qualsiasi violazione delle BCR commessa dallo stesso Esportatore di dati o da un Importatore di dati che abbia ricevuto i Dati personali trasferiti dal SEE in virtù di un Trasferimento pertinente o Trasferimento Successivo che abbia origine dal relativo Esportatore di dati del SEE.

Ai sensi degli Articoli IX (2) e (3), ogni Società AXA impattata dalle BCR sarà responsabile della perdita o del danno conseguente alla sua violazione delle BCR nei limiti previsti dalla legge e dalla regolamentazione applicabile. Una Società AXA impattata dalle BCR non sarà responsabile delle violazioni commesse da qualsiasi altra Società AXA impattata dalle BCR, salvo in caso di violazione da parte dell'Importatore di dati in cui l'Esportatore di dati possa indennizzare l' Interessato della Giurisdizione regolamentata (ai sensi degli Articoli IX(2) e (3)), e poi possa richiedere il rimborso all'Importatore di dati; per es. se un Importatore di dati viola le BCR e l'Esportatore di dati paga i danni al Soggetto interessato di una Giurisdizione regolamentata in relazione a tale violazione, l'Importatore di dati sarà poi tenuto a rimborsare l'Esportatore di dati. Analogamente, qualora un Esportatore di dati violi le BCR e l'Importatore di dati paghi i danni al Soggetto interessato della Giurisdizione regolamentata in relazione a tale violazione, l'Esportatore di dati sarà poi tenuto a rimborsare l'Importatore di dati.

L'Esportatore di dati che sia responsabile in seguito a una violazione da parte di un Importatore di dati può adottare le misure necessarie a porre rimedio a tali violazioni da parte dell'Importatore di dati e, considerando la violazione e il danno subito dal Soggetto interessato di una Giurisdizione regolamentata, indennizzare quest'ultimo conformemente alla legge applicabile e agli standard locali. Successivamente, l'Esportatore di dati può presentare ricorso contro l'Importatore di dati per la violazione delle BCR. L'Esportatore di dati può essere esonerato in tutto o in parte se può dimostrare di non essere responsabile della causa di tale danno.

Il Soggetto interessato di una Giurisdizione regolamentata ha diritto di ottenere l'indennizzo per i danni causati da un Importatore di dati in relazione ai Dati personali trasferiti dall'Esportatore di dati in considerazione della violazione subita e conformemente alla legge

applicabile, agli standard locali ed al danno subito (dimostrato). Nella misura consentita dalla giurisdizione applicabile, un Soggetto interessato di una Giurisdizione regolamentata ha diritto di presentare reclamo dinanzi all'Autorità per la Protezione dei dati o alle giurisdizioni competenti del paese in cui ha sede l'Esportatore di dati. Qualora quest'ultimo non abbia sede nel SEE ma tratti nel SEE Dati personali di un Soggetto interessato del SEE, la giurisdizione competente sarà nel paese in cui tale trattamento avviene. Qualora i Dati personali del Soggetto interessato del SEE abbiano origine da un Esportatore di dati del SEE, la giurisdizione competente sarà il luogo in cui ha sede l'Esportatore di dati del SEE.

2. Ulteriori disposizioni nei casi in cui l'Importatore di dati è Titolare

Le seguenti disposizioni si applicano soltanto nei casi in cui l'Importatore di dati agisce in qualità di Titolare e stabiliscono le uniche circostanze in cui un Interessato di una Giurisdizione regolamentata può presentare un reclamo contro tale Importatore di dati.

In situazioni in cui vengano presentati reclami sostenendo che l'Importatore di dati non abbia ottemperato agli obblighi delle BCR, il Soggetto interessato di una Giurisdizione regolamentata deve innanzitutto richiedere che il relativo Esportatore di dati adotti ragionevoli provvedimenti per indagare sulla questione e (qualora sussista una violazione) ponga rimedio al danno risultante dalla presunta violazione e subito dal Soggetto interessato di una Giurisdizione regolamentata e far valere i suoi diritti nei confronti dell'Importatore di dati che ha violato le BCR. Qualora l'Esportatore di dati non adotti tali provvedimenti entro un tempo ragionevole (normalmente 1 mese), il Soggetto interessato della Giurisdizione regolamentata avrà poi diritto a far valere i suoi diritti direttamente nei confronti dell'Importatore di dati. Un Soggetto interessato di una Giurisdizione regolamentata ha anche diritto ad agire direttamente contro un Esportatore di dati che non abbia compiuto i ragionevoli sforzi per stabilire se l'Importatore di dati sia in grado di adempiere i suoi obblighi in virtù delle presenti BCR nei limiti previsti dalla e conformemente alla legge applicabile.

3. Ulteriori disposizioni nei casi in cui l'Importatore di dati è Responsabile

Le seguenti disposizioni si applicano soltanto nei casi in cui l'Importatore di dati agisce in qualità di Responsabile e stabiliscono le uniche circostanze in cui un Interessato di una Giurisdizione regolamentata può presentare un reclamo contro tale Importatore di dati o il suo subappaltatore.

Qualora un Soggetto interessato di una Giurisdizione regolamentata non sia in grado di presentare una richiesta di indennizzo all'Esportatore di dati, derivante da una violazione da parte dell'Importatore di dati o del suo subappaltatore di qualsiasi suo obbligo in virtù delle presenti BCR, poiché l'Esportatore di dati è di fatto scomparso, ha cessato di esistere giuridicamente o è diventato insolvente, l'Importatore di dati accetta che il Soggetto interessato della Giurisdizione regolamentata possa presentare la richiesta all'Importatore di dati come se fosse l'Esportatore di dati, a meno che un successore non abbia assunto tutti gli obblighi giuridici dell'Esportatore di dati per contratto o per legge, nel qual caso il Soggetto interessato della Giurisdizione regolamentata potrà far valere i propri diritti contro tale successore. L'Importatore di dati non può basarsi su una violazione dei propri obblighi da parte di un subappaltatore al fine di evitare le proprie responsabilità.

Qualora un Interessato di una Giurisdizione regolamentata non sia in grado di presentare una richiesta di indennizzo all'Esportatore di dati o all'Importatore di dati, derivante da una violazione, da parte di una Società AXA subappaltatrice ed impattata dalle BCR, di qualsiasi suo obbligo in virtù delle presenti BCR, poiché l'Esportatore di dati e l'Importatore di dati sono di fatto scomparsi, hanno cessato di esistere giuridicamente o sono diventati insolventi, la Società AXA subappaltatrice ed impattata dalle BCR accetta che il Soggetto interessato della Giurisdizione regolamentata possa presentare la richiesta alla Società AXA subappaltatrice ed impattate dalle BCR in relazione alle sue attività di trattamento come se fosse l'Esportatore di

dati o l'Importatore di dati, a meno che un successore non abbia assunto tutti gli obblighi giuridici dell'Esportatore di dati o dell'Importatore di dati per contratto o per legge, nel qual caso il Soggetto interessato della Giurisdizione regolamentata può far valere i propri diritti contro tale successore. La responsabilità della Società AXA subappaltatrice ed impattata dalle BCR sarà limitata alla sua attività di trattamento di Dati personali.

ARTICOLO X - ASSISTENZA RECIPROCA E COLLABORAZIONE CON LE AUTORITÀ PER LA PROTEZIONE DEI DATI.

1. Collaborazione con le Autorità per la protezione dei dati

Le Società AXA impattate dalle BCR collaboreranno con la competente Autorità per la protezione dei dati per qualsiasi questione relativa all'interpretazione delle BCR, entro limiti coerenti con la legge e i regolamenti applicabili, e senza rinunciare a qualsiasi difesa e/o diritto di appello disponibile al Titolare:

- mettendo a disposizione il personale necessario per dialogare con le Autorità per la protezione dei dati,
- esaminando attivamente e valutando qualsiasi decisione presa dall'Autorità per la protezione dei dati e i pareri del Comitato europeo della Protezione dei Dati in relazione alle BCR,
- comunicando qualsiasi cambiamento sostanziale delle BCR alle rispettive Autorità per la protezione dei dati,
- rispondendo alle richieste di informazioni o ai reclami delle Autorità per la protezione dei dati
- applicando le pertinenti raccomandazioni e consigli della competente Autorità per la protezione dei dati in relazione alla conformità della Società AXA impattate dalle BCR alle BCR.

Le Società AXA impattate dalle BCR accettano di rispettare la decisione formale della competente Autorità per la protezione dei dati relativa all'interpretazione e applicazione delle presenti BCR, entro limiti coerenti con la legge e i regolamenti applicabili, e senza rinunciare a qualsiasi difesa e/o diritto di appello disponibile al Titolare.

2. Rapporto tra le leggi applicabili e le BCR

Le Società AXA impattate dalle BCR devono sempre ottemperare alle leggi locali applicabili. Qualora non esista una legge sulla protezione dei dati, i Dati personali saranno trattati conformemente alle BCR. Qualora la legge locale preveda un livello superiore di protezione dei Dati personali rispetto alle BCR, si seguirà la legge locale. Qualora la legge locale preveda un livello inferiore di protezione dei Dati personali rispetto alle BCR, si seguiranno le BCR.

Nel caso in cui una Società AXA impattata dalle BCR abbia motivo di ritenere che i requisiti di leggi/regolamenti applicabili impediscano alla Società stessa di ottemperare alle BCR, la Società AXA impattata dalle BCR informerà tempestivamente il DPO, il quale informerà il DPO dell'Esportatore di dati e il GDPO.

Nella misura in cui determinate parti delle presenti BCR siano in conflitto con i requisiti di legge applicabili, questi ultimi prevarranno finché i rispettivi conflitti non siano stati risolti in modo debitamente coerente con tutti i requisiti di legge applicabili. Il GDPO e/o il DPO possono contattare la competente Autorità per la protezione dei dati per discutere le potenziali soluzioni.

3. Richiesta di divulgazione da parte di organismi preposti all'applicazione della legge

Quando una Società AXA impattata dalle BCR riceve da parte di un'autorità preposta all'applicazione della legge o di un organismo responsabile della sicurezza nazionale una

richiesta legalmente vincolante di divulgazione di Dati personali che potrebbe avere un effetto negativo sulle garanzie fornite dalle BCR, la competente Autorità per la protezione dei dati sarà informata dal DPO o dal GDPO, tranne qualora sia proibito conformemente alle leggi locali applicabili. Le informazioni al DPA devono comprendere informazioni sui dati richiesti, sull'organismo richiedente e sulle basi legali della divulgazione.

Laddove la notifica delle richieste di divulgazione sia proibita secondo le leggi locali applicabili, la Società AXA impattata dalle BCR a cui è stata presentata la richiesta cercherà al meglio delle proprie possibilità di derogare da questa proibizione. Qualora malgrado gli sforzi non sia possibile derogare dalla proibizione, la Società AXA impattata dalle BCR che ha ricevuto la richiesta deve fornire alla competente Autorità per la protezione dei dati informazioni generali annuali in base alle richieste ricevute.

La divulgazione di Dati personali da parte di una Società AXA impattata dalle BCR a qualsiasi autorità pubblica deve comunque essere conforme ai principi di trattamento specificati in dettaglio nell'Articolo IV e non può essere massiccia, sproporzionata e indiscriminata in misura tale da eccedere quanto sia necessario in una società democratica.

ARTICOLO XI - DATA DI DECORRENZA e DURATA DELLE BCR

Le BCR entreranno in vigore il giorno 15 gennaio 2014 per un periodo di tempo illimitato.

Le BCR saranno applicabili a ogni Società AXA impattata dalle BCR dalla Data di Decorrenza dell'IGA stipulato in relazione alle presenti BCR. Le BCR cesseranno di essere applicabili a una determinata Società AXA impattata dalle BCR non appena (i) vengano risolte mediante comunicazione scritta del GDPO al DPA coordinatore (CNIL) e a ogni Società AXA impattata dalle BCR; o (ii) l'IGA stipulato venga risolto in base alle condizioni definite nello stesso.

ARTICOLO XII - LEGGE APPLICABILE – FORO COMPETENTE

1. Legge applicabile

Le presenti BCR (ivi compreso qualsiasi Contratto ad esse relativo) saranno lette e interpretate conformemente alla legge francese.

2. Controversie tra l'Importatore di dati e l'Esportatore di dati.

Qualsiasi controversia che dovesse insorgere tra l'Importatore di dati e l'Esportatore di dati in virtù del presente Contratto BCR sarà risolta dal tribunale competente del paese dell'Esportatore di dati, salvo diversamente previsto dalle leggi locali.

3. Altre controversie tra Società AXA impattate dalle BCR

Qualsiasi altra controversia che dovesse insorgere tra le Società AXA impattate dalle BCR in virtù delle BCR stesse (ivi compreso qualsiasi Contratto ad esse relativo) sarà risolta dai tribunali competenti di Parigi, salvo altrimenti previsto da un requisito obbligatorio delle leggi applicabili.

4. Controversie con Soggetti interessati di Giurisdizioni regolamentate

Nei limiti consentiti dalla giurisdizione applicabile e dalle disposizioni sui diritti di terze parti delle presenti BCR, un Soggetto interessato di una Giurisdizione regolamentata ha diritto a presentare un reclamo contro una Società AXA impattata dalle BCR o

(i) dinanzi alle giurisdizioni competenti di un paese SEE a scelta del Soggetto interessato: il Soggetto interessato può scegliere di agire avanti le autorità giudiziarie del paese SEE in cui l'Esportatore di dati ha una sede o avanti le autorità giudiziarie del paese SEE in cui il Soggetto interessato aveva la propria residenza abituale al momento dell'acquisizione dei Dati personali interessati dal reclamo; o

(ii) i tribunali di Parigi.

ARTICOLO XIII - AGGIORNAMENTO DELLE REGOLE

Il GDPO provvederà a riesaminare e aggiornare regolarmente le BCR, per esempio in seguito a importanti cambiamenti della struttura aziendale e del contesto normativo.

Tutte le Società AXA impattate dalle BCR accettano e riconoscono espressamente che:

- Le modifiche sostanziali a queste BCR, che incrementano notevolmente gli obblighi delle Società AXA impattate dalle BCR, possano essere approvate in una decisione dell'***AXA BCR Steering Committee*** dopo una consultazione di un (1) mese via email delle Società AXA impattate dalle BCR attraverso le email dei DPO note al GDPO; e

- Le modifiche non sostanziali alle presenti BCR, ossia tutte le altre modifiche, possono essere approvate in una decisione dell'***AXA BCR Steering Committee*** senza bisogno di consultare alcuna delle Società AXA impattate dalle BCR.

Il GDPO sarà incaricato di elencare le Società AXA impattate dalle BCR e controllare e documentare qualsiasi aggiornamento delle BCR e delle Società AXA impattate dalle BCR. Il GDPO comunicherà ogni anno tali Società AXA impattate dalle BCR aggiornate e qualsiasi modifica sostanziale delle BCR all'Autorità per la protezione dei dati coordinatrice e inoltre, su richiesta, a qualsiasi altra pertinente Autorità per la protezione dei dati. Il GDPO comunicherà senza indugio all'Autorità per la protezione dei dati coordinatrice qualsiasi cambiamento che inciderebbe materialmente sul livello di protezione offerto dalle BCR o influirebbe in modo significativo sulle BCR. Il DPO comunicherà su richiesta tale versione pubblica aggiornata delle BCR al Soggetto interessato della Giurisdizione regolamentata.

ELENCO DELLE APPENDICI:

Appendice 1: Contratto BCR
Appendice 2: Programma di verifica della conformità
Appendice 3: Data Protection Corporate Agreement

Omissis