Gruppo Bancario Igea Banca

POLICY DI GRUPPO

SULLA PROTEZIONE DEI DATI PERSONALI

CODICE: (GRU)-GOV-DNV-PDP-01

Area	**Processi di Governo (GOV)**
Macro-Ambito	**Disposizione Normative di Vigilanza (DNV)**
Ambito	**Privacy**
Perimetro di applicabilità	**Gruppo Bancario**
Data creazione	**28/01/2021**
Tipologia di documento	**Policy**
Data ultima approvazione CdA Banca del fucino	**28/01/2021**
Data recepimento Igea Digital Bank	**02/02/2021**

INDICE

1 PREMESSE, DEFINIZIONI E PRINCIPI GENERALI

La presente Policy sulla Protezione dei Dati Personali (la "Policy") definisce le linee guida alle quali le Società facenti parte del Gruppo Igea Banca devono attenersi per assicurare la tutela dei dati personali secondo i requisiti previsti dalla normativa in materia e in particolare al Regolamento (UE) 2016/679 in materia di protezione dei dati personali (di seguito anche "GDPR") e delle relative norme nazionali vigenti in materia.

L'entrata in vigore del Regolamento UE 2016/679 ("GDPR"), pubblicato in Gazzetta Ufficiale UE il 4 maggio 2016, ha abrogato la precedente Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, mentre l'emanazione del d.lgs. 101/2018, decreto di armonizzazione della normativa italiana al GDPR, ha modificato il Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (il "**Codice *Privacy***").

Con riferimento alla tutela dei dati personali, sono state, inoltre, emesse linee guida e di indirizzo da parte dello European Data Protection Board ("**EDPB**" già "**WP 29**") e del Garante per la Protezione dei Dati Personali (il "**Garante**").

Tra le principali novità, il GDPR ha:

- armonizzato la disciplina sulla protezione dei dati personali all'interno di tutta l'Unione europea;
- attribuito fondamentale importanza ai principi della accountability, della privacy by design e by default;
- coerentemente con il principio della accountability, introdotto, inter alia, gli istituti del Registro dei trattamenti, della valutazione d'impatto sulla protezione dei dati e della data breach notification;
- rafforzato e introdotto nuovi diritti degli interessati, che le imprese sono tenute a garantire al fine di assicurare che il trattamento dei dati personali sia svolto in piena conformità alla normativa, anche per incrementare il livello dei servizi forniti ai clienti;
- introdotto la figura del Data Protection Officer;
- inasprito le sanzioni amministrative pecuniarie che, nei casi delle violazioni ritenute più gravi, possono arrivare sino ad un massimo di € 20.000.000 o al 4% del fatturato globale annuo del Gruppo.

La Banca del Fucino (la "**Capogruppo**") emana la presente Policy per tutte le Società del Gruppo (le "**Società del Gruppo**" o, singolarmente, la "**Società del Gruppo**").

I contenuti della presente Policy e i successivi aggiornamenti sono di responsabilità del Consiglio di Amministrazione della Capogruppo (il "**CdA**") con il supporto del Data Protection Officer di Gruppo (il "**DPO**").

La Capogruppo e tutte le Società del Gruppo si attengono ai principi generali indicati nella presente Policy che provvedono a far valutare ed approvare dal proprio Consiglio di Amministrazione e in caso di aggiornamento si impegnano a fare approvare le modifiche.

Vista la complessità dell'attività svolta, nel rispetto delle esigenze delle singole Società, viene sottoposto all'approvazione del CdA della Capogruppo uno Schema di Regolamento sulla protezione dei dati personali (lo "**Schema di Regolamento**") che esprime, pur nel rispetto delle caratteristiche delle singole Società, criteri di comportamento coerenti con quelli individuati dalla presente Policy. Rimane in capo alle Società del Gruppo l'adozione di un autonomo Regolamento sulla protezione dei dati personali (il "**Regolamento**"), che dovrà essere deliberato dai rispettivi Consigli di Amministrazione sulla base dello specifico Schema di Regolamento allegato.

Al DPO di Gruppo è attribuita la responsabilità di:

- diffondere la Policy all'interno delle Società del Gruppo, monitorandone il recepimento da parte dei rispettivi Consigli di Amministrazione e l'osservanza da parte del personale;
- verificare che i contenuti della Policy e dei Regolamenti in materia di protezione dei dati personali (Normativa interna) risultino in linea con la normativa esterna tempo per tempo vigente;

- supportare le funzioni aziendali (quali le strutture operative: Business Unit, Servizi e relativi uffici centrali) nella corretta interpretazione dei principi contenuti nella normativa interna, fornendo consulenza ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR;
- raccogliere dalle singole funzioni aziendali competenti le segnalazioni di aggiornamento necessarie al conseguente adeguamento della presente Policy e della normativa interna;
- cooperare con l'Autorità di controllo e fungere da punto di contatto per l'Autorità stessa per questioni connesse al trattamento dei dati personali.

1.1 Definizioni

Per una più agevole comprensione della Policy si riportano di seguito le definizioni dei termini maggiormente utilizzati:

- "**dato personale**": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**interessato**"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale – articolo 4, punto 1), GDPR;
- "**categorie particolari di dati personali**": dati personali che rivelino 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 – articolo 9 GDPR;
- "**trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione – articolo 4, punto 2), GDPR;
- "**registro dei trattamenti**": i titolari e i responsabili del trattamento devono tenere un registro delle attività di trattamento svolte sotto la propria responsabilità, contenenti le informazioni elencate all'articolo 30 GDPR;
- "**limitazione di trattamento**": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro – articolo 4, punto 3), GDPR;
- "**profilazione**": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica – articolo 4, punto 4), GDPR;
- "**titolare del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione europea o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione europea o degli Stati membri – articolo 4, punto 7), GDPR;
- "**responsabile del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento – articolo 4, punto 8), GDPR;
- **Data Protection Officer ("DPO"):** il DPO o Responsabile della Protezione dei Dati, è il soggetto designato dal Titolare o dal Responsabile del Trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR - art. 37 GDPR;

- "**incaricato del trattamento**": le persone fisiche autorizzate a compiere operazioni di trattamento sotto l'autorità diretta del titolare o del responsabile del trattamento - art. 29 GDPR;
- "**delegato del titolare**": la persona fisica a cui il titolare delega l'esercizio di determinati adempimenti relativi alla protezione dei dati personali";
- **"principio di accountability"**: impone al titolare di mettere in atto le misure tecniche e organizzative adeguate al fine di garantire e dimostrare che il trattamento è effettuato conformemente alle disposizioni del GDPR tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche;
- **"principio di privacy by design"**: prescrive al titolare di adottare sia al momento della determinazione dei mezzi del trattamento (cfr. supra definizione di trattamento) che all'atto del trattamento stesso, misure tecniche e organizzative adeguate a garantire il rispetto del GDPR e la tutela dei diritti e delle libertà degli interessati (ad esempio, prevedendo tecniche di "data minimization");
- **"principio di privacy by default"**: richiede al titolare di predisporre misure tecniche e organizzative tali da garantire che, per impostazione predefinita, siano trattati esclusivamente i dati personali necessari a ogni specifica finalità del trattamento. Tale principio può essere declinato riducendo la quantità di dati raccolti, la portata del trattamento, il periodo di conservazione e il numero di soggetti che ha accesso ai dati personali;
- **"data breach" o "violazione di dati personali"**: 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; in caso di violazione dei dati personali, il titolare del trattamento deve notificare la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza, salvo che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione anche all'interessato senza ingiustificato ritardo;
- **"valutazione di impatto sulla protezione dei dati" o "DPIA"**: valutazione di impatto effettuata dal titolare quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

1.2 Principi Generali

La Capogruppo e le Società del Gruppo si impegnano a rispettare i principi generali applicabili al trattamento (articolo 5 del GDPR), in base ai quali i dati personali devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**principio di liceità, correttezza e trasparenza**);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo non incompatibile con tali finalità (**principio di limitazione della finalità**);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**principio di minimizzazione dei dati**);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**principio di esattezza**);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**principio di limitazione della conservazione**);
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (**principi di integrità e riservatezza**).

Il Titolare del trattamento (la Capogruppo e le Società del Gruppo) è competente per il rispetto dei principi sopra riportati ed è in grado di comprovarlo («responsabilizzazione»).

Ai sensi dell'articolo 6 del GDPR, il trattamento è lecito solo se ricorre almeno una delle seguenti condizioni:

- l'interessato ha espresso il proprio consenso;
- il trattamento è necessario per eseguire un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere ad un obbligo di legge;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- 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;
- il trattamento è necessario per perseguire un legittimo interesse del titolare o di terzi, salvo che prevalgano gli interessi o i diritti e le libertà dell'interessato.

1.3 Aggiornamenti in materia di protezione dei dati personali

Nel caso in cui intervengano novità normative e/o modifiche della struttura aziendale, la **normativa interna** - inclusa la presente Policy - deve essere prontamente aggiornata per recepirle.

La Capogruppo e le Società del Gruppo assicurano l'aggiornamento della **documentazione privacy**, ivi incluse le informative e i moduli di consenso rilasciati agli interessati, prevedendo appositi meccanismi di verifica e aggiornamento periodici. In particolare, è previsto che nelle informazioni rese dai vari soggetti ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679 sia inserita la data del relativo aggiornamento, da verificare periodicamente.

A tal fine, deve essere stabilito un flusso di informazioni adeguato verso la Funzione deputata agli aggiornamenti della documentazione privacy in modo da garantire che questa sia informata di ogni novità che necessita di essere recepita nella documentazione privacy stessa.

In ogni caso, tale Funzione deve spontaneamente verificare l'adeguatezza della documentazione privacy alla normativa vigente, ai trattamenti svolti e alle prassi aziendali almeno una volta all'anno.

La Capogruppo e le Società del Gruppo prevedono meccanismi interni di controllo e revisione dei **dati personali trattati**, in modo da garantire che essi siano sempre esatti e aggiornati, nonché adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento perseguite e comunicate agli interessati.

Devono essere cancellati o resi anonimi i dati personali per i quali non è più necessaria e/o possibile la conservazione, anche alla luce delle informazioni rilasciate agli interessati tramite informativa.

2 GESTIONE DEI TRATTAMENTI

2.1 Condizioni di liceità del trattamento

La Capogruppo e le Società del Gruppo assicurano che i dati personali degli interessati siano trattati esclusivamente in presenza di una delle condizioni di liceità del trattamento previste dal GDPR, tenendo in considerazione la natura del dato personale oggetto di trattamento (i.e. dati comuni, categorie particolari di dati personali, dati giudiziari e dati di minori).

La Capogruppo e le Società del Gruppo, nel dare avvio a ogni nuova tipologia di trattamento, assicurano, ove necessario con il coinvolgimento del DPO di Gruppo, che esso sia fondato su una delle fonti di liceità del trattamento previste dal GDPR.

La Capogruppo e le Società del Gruppo forniscono alle persone autorizzate e incaricate al trattamento che interagiscono con gli interessati le istruzioni necessarie a garantire il rispetto della normativa e della presente Policy.

Qualora il fondamento di liceità del trattamento sia il **consenso**, gli incaricati devono rilasciare un'informativa agli interessati e richiedere il consenso, nel rispetto delle procedure interne e delle istruzioni ricevute, prima che il trattamento abbia inizio. Il consenso deve essere libero, specifico e informato, manifestato tramite un'azione positiva inequivocabile e richiesto separatamente per ogni finalità del trattamento.

La normativa interna stabilisce l'obbligo di registrare l'ottenuto consenso tramite processi che assicurino un agevole recupero della data, modalità e contenuto del consenso.

I termini del trattamento, indicati sulle informative, contengono e descrivono in modo puntuale il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

2.2 Trattamento di dati di minori e di categorie particolari di dati personali

Nel caso in cui il trattamento sia basato sul consenso e abbia ad oggetto dati personali di minori, la Capogruppo e le Società del Gruppo assicurano che il trattamento abbia luogo esclusivamente nel caso in cui tale consenso sia prestato o autorizzato dal titolare della potestà genitoriale.

Il consenso o l'autorizzazione del titolare della responsabilità genitoriale sono registrati tramite processi che ne assicurino un agevole recupero.

Qualora il trattamento riguardi categorie particolari di dati personali, la Capogruppo e le Società del Gruppo rispettano le condizioni di liceità previste all'articolo 9 GDPR. In particolare, quando il trattamento di categorie particolari di dati personali si basa sul consenso, è rilasciata un'informativa agli interessati ed è richiesto loro un consenso esplicito, nel rispetto delle procedure interne e delle istruzioni ricevute, prima che il trattamento abbia inizio.

2.3 Gestione del Registro dei trattamenti

La Capogruppo e le Società del Gruppo gestiscono la tenuta, l'aggiornamento e la conservazione del Registro dei Trattamenti nel rispetto della normativa di riferimento e della presente Policy.

Dovrà essere previsto un flusso informativo da parte di tutte le funzioni aziendali alla Funzione responsabile per la tenuta e l'aggiornamento del Registro dei Trattamenti, dovendo essere tempestivamente segnalate, inter alia:

- la progettazione di una nuova iniziativa che preveda il trattamento di dati personali;
- l'estensione di un trattamento già previsto a nuove categorie di interessati o dati personali;
- qualsiasi modifica della struttura organizzativa della Società;
- la sottoscrizione di contratti di fornitura che comportino la nomina a responsabile esterno della controparte;
- le categorie di destinatari cui i dati personali oggetto del trattamento sono comunicati;
- la necessità di trasferire i dati personali trattati all'esterno dell'Unione europea;
- qualsiasi modifica dei sistemi informativi adottati;
- l'adozione di nuove misure tecniche e/o organizzative.

Deve altresì essere previsto il dovere della Funzione predisposta alla tenuta, aggiornamento e conservazione del Registro dei Trattamenti, indipendentemente dallo spontaneo flusso informativo, di interrogare le funzioni aziendali almeno una volta all'anno per verificare il corretto aggiornamento del Registro dei Trattamenti alla luce dei trattamenti svolti dalla Capogruppo e dalle Società del Gruppo.

Il Registro aggiornato può essere reso disponibile ai dipendenti della Capogruppo e delle Società del Gruppo che ne facciano richiesta, adesempio per conoscere i trattamenti effettuati nell'ambito della Funzione di appartenenza, secondo modalità atte ad assicurarne l'agevole consultazione.

3 MODELLO DI NOMINA E DI CONTRATTO

3.1 Incaricati al Trattamento e Referenti Privacy

La Società prevede procedure interne per la nomina di tutti i dipendenti che trattano dati personali ad incaricati sotto la diretta autorità del Titolare e per la nomina di un referente interno delle attività in materia di privacy ("Referente Privacy"), al quale saranno affidate mansioni specifiche ai fini privacy, nel rispetto delle normative in materia (cfr. l'art. 29 del GDPR e l'art. 2-quaterdecies del Codice Privacy, come modificato dal d.lgs. 101/2018).

È necessario garantire una formazione adeguata agli incaricati e al Referente Privacy tramite l'erogazione di corsi e la fornitura di istruzioni precise su come effettuare i trattamenti. A questo riguardo, il Titolare del trattamento organizza eventi di formazione in materia di protezione dei dati personali, aventi ad oggetto la normativa di riferimento vigente e la struttura privacy adottata. Questi eventi formativi dovranno essere organizzati in modo periodico e, in ogni caso, qualora dovessero intervenire novità normative o organizzative rilevanti. La formazione erogata è controllata dal DPO di Gruppo.

3.2 Responsabili del trattamento e contitolari del trattamento

Il titolare del trattamento può **esternalizzare** alcuni trattamenti ad un responsabile del trattamento, che dovrà essere selezionato sulla base della sua capacità di offrire garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate al rispetto dei requisiti del GDPR.

Ogni qualvolta un trattamento è esternalizzato ad una persona fisica o giuridica, il titolare assicura che tale soggetto terzo sia nominato responsabile del trattamento nel rispetto delle disposizioni del GDPR.

In **fase di selezione** del responsabile esterno, deve essere assicurato che questi rispetti tutte le garanzie previste dall'articolo 28 GDPR e, in particolare, che presenti garanzie sufficienti in merito all'adozione di misure tecniche e organizzative adeguate a tutelare i diritti degli interessati.

Una volta selezionato il responsabile nel rispetto della presente Policy, si provvede alla relativa **designazione** tramite la conclusione di un contratto di nomina che presenti tutti gli elementi richiesti dal GDPR, tra cui precise istruzioni cui il responsabile dovrà attenersi e il diritto della Società di risolvere il contratto in caso di inadempimento della controparte.

Nel corso di tutta la relazione contrattuale con il responsabile, dovrà essere assicurato un **monitoraggio**, prevedendo verifiche periodiche sull'operato dei responsabili esterni al fine di appurare il rispetto della normativa e delle istruzioni impartite. A tal fine, potrà essere sollecitato l'invio di rendiconti, la compilazione di questionari e/o potranno essere effettuate delle visite ispettive presso il responsabile anche coinvolgendo, qualora necessario, esperti in materia informatica.

Nel caso in cui dovessero emergere alcune criticità, dovrà essere coinvolto il DPO di Gruppo per valutare i necessari interventi di mitigazione delle stesse. Qualora le criticità dovessero perdurare o fossero di un'entità tale da giustificare la cessazione del rapporto contrattuale, la Capogruppo e le Società del Gruppo dovranno valutare l'eventuale interruzione della relazione contrattuale con il responsabile.

Qualora venga nominato un nuovo responsabile o vengano modificati i responsabili esistenti, deve essere aggiornato conseguentemente anche il Registro dei trattamenti (si veda il punto 2.3 della presente Policy).

Nel caso in cui la Capogruppo o una Società del Gruppo sia designata - previa analisi della richiesta da parte del Referente Privacy, che coinvolge il DPO di Gruppo ed eventuale approvazione da parte dell'Organo decisionale - quale Responsabile del trattamento da parte di un altro soggetto, interno o esterno al Gruppo (ad esempio una Compagnia di Assicurazione della quale si promuovono i prodotti), viene verificata l'applicazione di tutti gli adempimenti derivanti da tale designazione.

Se per uno o più trattamenti di dati personali le finalità o i mezzi utilizzati sono determinati congiuntamente dal titolare (Capogruppo o la Società del Gruppo) e altri soggetti (contitolari del trattamento), le norme interne prevedono la definizione di un accordo nel quale i contitolari indichino le rispettive responsabilità in merito all'osservanza degli

obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti da parte dell'interessato e alla resa dell'informativa di cui agli articoli 13 e 14 del GDPR. Il contenuto essenziale dell'accordo è messo a disposizione degli interessati, nelle forme individuate con l'intervento del DPO di Gruppo.

4 PRIVACY BY DESIGN/DEFAULT

4.1 Accountability

Per trattare i dati personali in conformità con la normativa vigente e la presente Policy, la Capogruppo e le Società del Gruppo adottano misure tecniche e organizzative adeguate e ne dispongono il costante aggiornamento. Devono, altresì, essere adottati adeguati meccanismi di controllo della costante conformità delle misure di sicurezza nel tempo, alla luce delle esigenze previste dalla normativa pro tempore vigente.

La Capogruppo e le Società del Gruppo sono tenute a documentare le attività svolte per garantire che i trattamenti siano effettuati in linea con la normativa applicabile ed a tenere tale documentazione a disposizione per eventuali accessi dell'Autorità Garante.

4.2 Privacy by design

La Capogruppo e le Società del Gruppo assicurano che tutte le applicazioni, servizi, prodotti ed attività che prevedono il trattamento di dati personali considerino il diritto alla protezione dei dati. Tutti i trattamenti sono progettati, e successivamente effettuati, tenendo in considerazione gli effetti che potrebbero avere sulla protezione dei dati personali e sui diritti degli interessati. A tal fine, sin dal momento della determinazione dei mezzi del trattamento sono adottate misure tecniche e organizzative adeguate, quali la pseudonimizzazione e la minimizzazione dei dati, volte ad attuare in modo efficace i principi di protezione dei dati e ad integrare nel trattamento le garanzie necessarie a soddisfare i requisiti della normativa applicabile e tutelare i diritti degli interessati.

4.3 Privacy by default

La Capogruppo e le Società del Gruppo assicurano che siano trattati, per impostazione predefinita, esclusivamente i dati necessari per ogni specifica finalità del trattamento.

A tal fine, in fase di delineazione del trattamento sono adottate le necessarie misure tecniche e organizzative e sono valutati, soprattutto, i seguenti elementi al fine di ridurre al minimo necessario alle finalità perseguite l'impatto sul diritto alla protezione dei dati: (i) quantità dei dati personali da raccogliere; (ii) portata del trattamento; (iii) il periodo di conservazione; (iv) numero di soggetti che ha accesso ai dati personali.

4.4 Trasferimento di dati personali verso Paesi Terzi o organizzazioni internazionali

Qualora la Capogruppo o una Società del Gruppo intenda trasferire i dati personali trattati all'esterno dell'Unione europea, una procedura interna deve assicurare la verifica del rispetto di almeno una delle condizioni previste dal GDPR per il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

In particolare, il trasferimento di dati personali all'esterno dell'Unione europea potrà avvenire, inter alia, in presenza di:

- una decisione di adeguatezza della Commissione;
- clausole tipo di protezione ("Model Contract Clauses") dei dati adottate dalla Commissione;
- clausole contrattuali tra il titolare del trattamento e il titolare/responsabile destinatario dei dati nel paese terzo approvate dall'autorità di controllo;
- un codice di condotta o un meccanismo di certificazione e il contestuale impegno del titolare/responsabile destinatario dei dati di applicare le garanzie adeguate.

Inoltre, il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale sarà possibile nel caso in cui:

- l'interessato abbia prestato esplicitamente il consenso dopo essere stato informato dei possibili rischi;
- il trasferimento sia necessario per l'esecuzione di un contratto concluso tra l'interessato e il titolare ovvero di misure precontrattuali adottate su istanza dell'interessato;
- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare e un terzo a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico.

Qualora il destinatario dei dati personali effettui trattamenti per conto del titolare, deve essere rispettato quanto previsto dalla sezione 3.2 della presente Policy sulla nomina dei responsabili del trattamento.

5 DIRITTI DEGLI INTERESSATI

5.1 I diritti subordinati a una richiesta espressa dell'interessato

I macro-processi per la gestione dei diritti degli interessati il cui soddisfacimento è subordinato a una richiesta dell'interessato sono riconducibili ai seguenti ambiti principali:

- ricezione della richiesta;
- gestione della richiesta;
- risposta all'interessato e archiviazione.

La Capogruppo e le Società del Gruppo regolano e gestiscono attraverso la normativa aziendale il riscontro della richiesta nei termini e alle condizioni per l'esercizio dei diritti stabiliti dal GDPR.

I diritti che il GDPR garantisce all'interessato sono:

1. **Diritto di Accesso**: l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali che comprendono i dati personali conferiti dall'interessati, i dati personali osservabili generati in esecuzione del contratto, i termini del trattamento compreso il periodo di conservazione previsto;
2. **Diritto di Rettifica**: l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
3. **Diritto di Cancellazione**: l'interessato ha il diritto di ottenere dal titolare del trattamento, se sussistono i motivi indicati dal GDPR, la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali;
4. **Diritto di limitazione di trattamento**: l'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando si verificano le ipotesi previste dall'Art. 18 del GDPR;
5. **Diritto di Opposizione / Revoca**: l'interessato ha il diritto di opporsi, o revocare il consenso, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
6. **Diritto alla Portabilità**: l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora il trattamento fosse stato effettuato con mezzi automatizzati.

Infine, nel caso di esercizio dei diritti di rettifica, cancellazione e/o limitazione del trattamento da parte dell'interessato, il Titolare provvede anche a effettuare la comunicazione prevista dall'articolo 19 GDPR.

5.1 I diritti non subordinati a una richiesta dell'interessato

Senza attendere la ricezione di una richiesta da parte dell'interessato, la Capogruppo e le Società del Gruppo si impegnano a garantire che:

- sia fornita idonea informativa all'interessato al momento della raccolta di dati personali presso lo stesso o, se i dati non sono raccolti direttamente presso l'interessato, entro i seguenti termini: a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato, oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali;
- l'interessato non sia sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incidano in modo analogo significativamente sulla sua persona; ciò fatti salvi i casi in cui la decisione a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione europea o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato.

6 MISURE DI SICUREZZA

La Capogruppo e le Società del Gruppo adottano misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche.

Tali misure devono essere altresì idonee a prevenire ogni violazione di dati personali, ivi incluse la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trattati. Qualora si verifichi una violazione di dati personali, le misure tecniche e organizzative adottate devono comunque essere idonee a consentire di individuare e contrastare l'avvenuta violazione.

7 LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, perché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, è necessario effettuare una valutazione dell'impatto prima di procedere al trattamento stesso.

Ogni qualvolta sia previsto un nuovo trattamento, sia modificato un trattamento esistente o comunque muti il rischio presentato da un trattamento svolto, la Capogruppo e le Società del Gruppo dovranno valutare la necessità o opportunità di effettuare una Data Protection Impact Assessment ("DPIA") in considerazione del rischio presentato dal trattamento e applicando la metodologia sviluppata a livello di gruppo.

Per i trattamenti già sottoposti a DPIA deve essere prevista una revisione di tali valutazioni almeno ogni 3 anni.

Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il DPO.

Qualora la DPIA evidenzi un rischio elevato per gli interessati, con il supporto del DPO, deve essere valutata l'adozione di ulteriori misure per attenuare il rischio e/o la necessità di effettuare una consultazione preventiva con il Garante. Eventuali successivi suggerimenti del Garante sono immediatamente recepiti prima di procedere al trattamento oggetto della DPIA.

8 DATA BREACH NOTIFICATION

Nel caso in cui si verifichi una violazione dei dati personali che presenti un rischio per le libertà e i diritti degli interessati, la Capogruppo e le Società del Gruppo devono prevedere modalità immediata di reazione in maniera da permettere:

(i) la notifica dell'avvenuta violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza e, se ricorrono i presupposti, all'interessato; ivi inclusa

(ii) l'adozione delle misure necessarie ad attenuare gli effetti negativi della violazione.

La Capogruppo e le Società del Gruppo tengono un registro delle violazioni e stabiliscono procedure interne che ne disciplinano l'aggiornamento al sussistere di ogni violazione, indifferentemente dal rischio presentato per i diritti e le libertà degli interessati e dalla eventuale notificazione all'Autorità di controllo.

In tale registro dovranno essere indicati tutti gli elementi richiesti dalla normativa vigente, tra cui: (i) le circostanze relative alla violazione; (ii) le sue conseguenze; (iii) le misure adottate per contrastarla e limitarne gli effetti; (iv) i dati personali coinvolti; (v) informazioni adeguate al fine di consentire al Titolare di determinare le motivazioni per non aver effettuato la notifica, o per averla effettuata in ritardo.

Inoltre, devono essere previsti meccanismi di conservazione di tutte le comunicazioni riguardanti la violazione.

9 IL SISTEMA DELLE RELAZIONI E DEI FLUSSI INFORMATIVI

9.1 Premessa

Devono essere definiti i flussi informativi volti ad assicurare agli Organi Aziendali e alle Funzioni di controllo della Capogruppo e delle Società del Gruppo la piena conoscenza e governabilità degli adempimenti in materia di protezione dei dati personali.

A tal fine, devono essere previsti canali di comunicazione efficaci per assicurare che il personale, a tutti i livelli, sia a conoscenza dei presidi di conformità relativi ai propri compiti e responsabilità.

Il sistema delle relazioni deve essere costituito sia da flussi informativi codificati derivanti da attività con periodicità definita e/o tempistica certa, sia da informative prodotte all'occorrenza che possono essere predisposte anche in maniera non strutturata.

9.2 Flussi informativi interni

Al fine di assicurare un set di flussi informativi e le relazioni tra le diverse strutture aziendali coinvolte nei processi di gestione in materia di protezione dei dati personali, devono essere garantite almeno le seguenti tipologie di scambi informativi tra il DPO di Gruppo e le diverse strutture aziendali coinvolte, nella Capogruppo e nelle Società del Gruppo, nei processi di gestione in materia di protezione dei dati personali:

- Reporting periodico verso gli Organi Aziendali che devono essere informati, almeno una volta l'anno, sullo svolgimento dei diversi macro-processi relativi alla protezione dei dati personali. In ogni caso, qualora siano riscontrate irregolarità o problematiche di particolare gravità (valutate di volta in volta dal DPO di Gruppo) deve essere fornita una pronta informazione agli organi aziendali;
- Flussi informativi tra il DPO di Gruppo e il Referente Privacy interno alla Capogruppo e alle Società del Gruppo, il quale riferisce, almeno annualmente e ad ogni caso all'occorrenza, al DPO di Gruppo in merito ai principali accadimenti in materia di protezione dei dati personali relativi ai trattamenti di propria competenza (ad es. tramite un apposito questionario o comunque in forma scritta);
- reporting costante verso il Referente Privacy interno, della Capogruppo e della Società del Gruppo (e, ove necessario direttamente al DPO di Gruppo) da parte delle Funzioni Aziendali, in merito ad ogni problematica

riscontrata inerente al trattamento dei dati personali;

- Il DPO di Gruppo può essere invitato a partecipare alle riunioni di eventuali Comitati, rilevanti in materia di controlli interni (quale ad es. il Comitato Rischi costituito in seno alla Capogruppo) nelle modalità previste dai relativi regolamenti.