Policy

in materia di protezione dei dati personali

- Delibera del Consiglio di Amministrazione del 02/05/2018

Indice

1) Premessa

1.1) Oggetto e scopo

La presente Policy sulla Protezione dei Dati Personali (la "Policy") definisce le linee guida alle quali la Banca (di seguito denominata "Titolare") deve attenersi nella pianificazione e nello svolgimento di qualsivoglia attività che implichi il trattamento di Dati personali per assicurare la tutela di tali Dati 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").
Le disposizioni della presente Policy hanno il fine di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche.
In particolare, la Policy individua:

- i destinatari della normativa interna ed esterna in materia di privacy;
- i principi generali a protezione dei Dati personali a cui è improntata l'attività aziendale;
- le modalità di aggiornamento e revisione della Policy;
- i principali ruoli previsti in ambito privacy;
- i processi sottesi a pianificazione e svolgimento di attività del Titolare che implicano il trattamento di Dati personali.

1.2) Contesto normativo di riferimento

Il 14 aprile 2016 il Parlamento e il Consiglio Europeo hanno approvato il Regolamento UE n. 679/2016 in materia di protezione dei Dati personali (di seguito "GDPR" e "Regolamento"), entrato in vigore il 25 Maggio 2016 e direttamente applicabile in tutta l'Unione Europea dal 25 Maggio 2018 con conseguente abrogazione della Direttiva 95/46/CE del Parlamento e del Consiglio Europeo del 24 Ottobre 1995, recepita in Italia dal Decreto Legislativo n. 196 del 30 Giugno 2003 (Codice in materia di protezione dei Dati personali).
Il GDPR modifica in maniera profonda la normativa in materia di privacy e in particolare:

- armonizza la disciplina sulla protezione dei Dati personali all'interno di tutta l'Unione europea;
- attribuisce fondamentale importanza ai principi della accountability, della privacy by design e by default;
- coerentemente con il principio della accountability, introduce, inter alia, gli istituti del Registro dei trattamenti, della valutazione d'impatto sulla protezione dei dati e della data breach notification;
- rafforza e introduce 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;
- introduce la figura del Data Protection Officer;
- inasprisce 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 a livello di gruppo imprenditoriale.

Il contesto normativo di riferimento comprende inoltre l'ulteriore normativa primaria e secondaria in materia privacy e protezione dei Dati personali, compresi i provvedimenti emanati dal Garante, dalle Istituzioni europee e dal WP29, nonché le norme previste del codice civile e penale italiano.

1.3) Principi generali

Il Titolare svolge le proprie attività nel rispetto dei principi generali in materia di privacy previsti dalla normativa di riferimento e dalla presente Policy.
In particolare, nella pianificazione o espletamento di qualsiasi attività che comporti trattamento di Dati personali, il Titolare assicura che i Dati personali siano:

- 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 personali**);
- esatti e, se necessario, aggiornati tempestivamente 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**).

1.4) Adozione e aggiornamento

La presente Policy è approvata dal Consiglio di Amministrazione su proposta del Data Protection Officer (il "DPO").
Il DPO verifica nel continuo e comunque con cadenza annuale la complessiva idoneità delle procedure predisposte al fine di assicurare il conseguimento degli obiettivi posti dalla disciplina vigente in materia, tenendo conto tra l'altro delle modifiche eventualmente intervenute nella normativa di riferimento, negli assetti organizzativi del Titolare nonché dell'efficacia dimostrata dalle procedure nella prassi applicativa.
A tal fine, sono previsti verso il DPO, in quanto funzione deputata all'aggiornamento della documentazione interna in materia di privacy, i flussi informativi descritti al successivo capitolo 11, finalizzati ad informarlo di ogni novità da cui potrebbe discendere la necessità di un aggiornamento della Policy e dell'ulteriore documentazione privacy.
La Funzione Compliance attesta la conformità della presente Policy alla normativa vigente rilevante ai fini della materia in oggetto.
Le Funzioni di Controllo, per quanto di rispettiva competenza, effettuano i controlli necessari a verificare l'effettivo rispetto della presente Policy.

1.5) Definizioni

Ai fini della presente Policy si intende per:

- "**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;
- "**Data breach**": 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;
- "**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;
- "**Data Protection Officer o DPO**": indica il soggetto designato dal Titolare o dal Responsabile del trattamento per assolvere funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR;
- "**Garante**": l'Autorità garante italiana per la protezione dei Dati personali;
- "**Incaricato**": la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- "**Limitazione di trattamento**": il contrassegno dei Dati personali conservati con l'obiettivo di limitarne il trattamento in futuro – articolo 4, punto 3), GDPR;
- "**Principio di accountability**": il principio che impone al titolare di mettere in atto le misure tecniche e organizzative adeguate per garantire e per 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 default**": il principio che 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, ad esempio 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;
- "**Principio di privacy by design**": il principio che prescrive al titolare di adottare sia al momento della determinazione dei mezzi del 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;
- "**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;
- "**Procedura**": il documento adottato dal Titolare al fine di disciplinare specifici processi interni;
- "**Referente privacy**": il soggetto interno alla realtà aziendale del Titolare che supporta il DPO nello svolgimento delle sue funzioni.
- "**Registro dei trattamenti**": i titolari e i Responsabili del trattamento devono tenere il registro delle attività di trattamento svolte sotto la propria responsabilità, contenenti le informazioni di cui all'articolo 30 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;
- "**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 o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri – articolo 4, punto 7), GDPR. Ai fini della presente Policy, il Titolare coincide con la Banca;
- "**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;
- "**Valutazione di impatto sulla protezione dei dati**" o "Data Protection Impact Assessment (DPIA)": valutazione di impatto sulla protezione dei dati effettuata dal titolare quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- "**WP29**": organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei Dati personali designate da ciascuno Stato membro dell'Unione Europea costituito ai sensi dell'articolo 29 della Direttiva CE 95/46.

1.6) Ambito di applicazione

Tutto il personale dipendente, i consulenti con contratto di collaborazione coordinata e continuativa, i collaboratori esterni occasionali, gli addetti alla manutenzione, gli stagisti e gli ulteriori collaboratori del Titolare a diverso titolo, sono tenuti a rispettare scrupolosamente la presente Policy nell'ambito delle rispettive competenze e attività.
Al fine di assicurare a tutti i destinatari la conoscenza dei principi, degli indirizzi e delle procedure adottati dal Titolare in conformità alla presente Policy, la stessa e i relativi aggiornamenti sono pubblicati nel Documentale.

2) DPO

Il DPO e la relativa struttura organizzativa rappresentano la principale funzione di consultazione, consulenza, sorveglianza e controllo in materia di protezione dei Dati personali.
Nell'espletamento delle proprie attribuzioni, il DPO si avvale inoltre della collaborazione del Referente Privacy.

2.1) Designazione

Avvalendosi della possibilità di nominare un DPO esterno prevista dall'articolo 37, comma 6 del GDPR, previa verifica del rispetto dei requisiti previsti dal GDPR con particolare riferimento ai requisiti di indipendenza e assenza di conflitti di interesse, il Consiglio di Amministrazione ha deliberato di nominare quale proprio DPO il DPO di Cassa Centrale.
La nomina del DPO è formalizzata tramite apposito atto di designazione che specifica l'ambito del suo mandato.
I dati di contatto del DPO sono comunicati agli interessati, al Garante e a tutto il personale, in modo tale da garantire che lo stesso possa essere contattato in qualsiasi momento.
Al Garante è comunicato altresì il nominativo del DPO.

2.2) Posizione

Il DPO:

- è interessato quando vengono prese decisioni con implicazioni sulle misure di protezione dei Dati personali;
- è coinvolto nel processo di definizione di nuovi prodotti, servizi, progetti di business e relaziona periodicamente in merito alla conformità dei trattamenti e all'andamento degli indicatori interni sulla protezione dei Dati personali;
- è facilmente raggiungibile, tramite mezzi sicuri di comunicazione, dagli interessati e all'interno dell'organizzazione aziendale, per tutte le questioni relative al trattamento dei loro Dati personali e ai loro diritti previsti dal GDPR;
- funge da punto di contatto per il Garante per questioni connesse al trattamento, tra cui la consultazione preventiva e consultazioni relative a qualunque altra questione.

2.3) Requisiti di idoneità

Il DPO è individuato in funzione delle sue qualità professionali e in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati personali; il livello necessario di conoscenza specialistica è determinato in base ai trattamenti di Dati effettuati e alla protezione necessaria per i Dati personali trattati dal Titolare o dal Responsabile del trattamento.
Il DPO è a conoscenza dello specifico settore di attività e della struttura organizzativa del Titolare e ha familiarità con le operazioni di trattamento, i sistemi informativi e le esigenze di sicurezza e protezione manifestate dal Titolare stesso.
In particolare il DPO, individuato in conformità alle disposizioni del GDPR e alle indicazioni del WP29, è in possesso dei seguenti requisiti:

- conoscenza ed esperienza sulla normativa privacy nazionale ed europea;
- competenze informatiche e conoscenza del sistema informativo aziendale;
- conoscenza del business del titolare;
- competenze relazionali;
- integrità ed elevati standard deontologici;
- indipendenza e assenza di qualsiasi conflitto di interesse con il ruolo svolto di DPO.

Ai fini del rispetto dei requisiti di indipendenza e assenza di conflitto di interesse, il DPO è individuato tra soggetti che non rivestano incarichi di alta direzione o abbiano poteri decisionali in ordine alle finalità e modalità del trattamento dei Dati personali con riferimento all'attività aziendale del Titolare o del Responsabile del trattamento.

2.4) Mansioni del DPO

Il GDPR attribuisce al DPO compiti di consulenza, informazione e sorveglianza, nonché un ruolo di contatto con il Garante e gli interessati, ammettendo la possibilità che gli siano attribuite mansioni ulteriori, purché non diano adito a conflitti di interesse.
Con riferimento alla Policy, al DPO è attribuita la responsabilità di:

- diffondere la Policy monitorandone il recepimento da parte del Consiglio di Amministrazione;
- verificare che i contenuti della Policy risultino in linea con la normativa interna ed esterna tempo per tempo vigente;
- supportare le funzioni aziendali del Titolare (strutture operative: Business Unit, Servizi e relativi uffici centrali) nella corretta interpretazione dei principi contenuti nella Policy;
- raccogliere dalle funzioni aziendali competenti le segnalazioni relative alla necessità di aggiornamento della Policy.

Le attività del DPO sono indicate nell'atto di designazione e riportate nell'**allegato 1** alla presente Policy.

3) Ruoli privacy

3.1) Referente privacy

Il Referente Privacy è nominato dal Consiglio di Amministrazione in funzione dell'esperienza professionale, delle competenze specialistiche in materia di protezione dei Dati personali nonché della conoscenza del business aziendale.
Il Referente privacy svolge un ruolo di collegamento tra il DPO, gli Incaricati e gli Organi Aziendali del Titolare e collabora con il DPO svolgendo le attività dettagliate nell'**allegato 2** alla presente Policy.

3.2) Incaricati al Trattamento

Il Titolare adotta delle procedure interne per la nomina ad Incaricati delle persone fisiche dallo stesso autorizzate a trattare Dati personali e per l'aggiornamento di tali nomine.
Il processo di nomina è disciplinato all'interno dell'apposita Procedura tempo per tempo aggiornata e pubblicata nel Documentale.
Il Titolare garantisce inoltre un'adeguata formazione degli Incaricati tramite corsi e la fornitura di istruzioni precise su come effettuare i trattamenti. A tal fine, il Titolare organizza eventi di formazione in materia di protezione dei Dati personali, sulla normativa applicabile e sull'impianto privacy adottato. Questi eventi formativi sono organizzati periodicamente e, in ogni caso, qualora dovessero intervenire novità normative o organizzative rilevanti.

3.3) Responsabili Esterni del Trattamento (Artt. 27 e 28 GDPR)

Il Titolare può esternalizzare alcuni trattamenti a soggetti individuati quali Responsabili del trattamento, selezionati tenendo in considerazione la 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 esterno del trattamento nel rispetto delle disposizioni del GDPR.
Una volta selezionato il Responsabile esterno nel rispetto della presente Policy, si provvede alla sottoscrizione di un contratto o diverso atto giuridico di nomina che presenti tutti gli elementi richiesti dal GDPR, tra cui precise istruzioni cui il Responsabile esterno dovrà attenersi e il diritto del Titolare di risolvere il contratto in caso di inadempimento della controparte.
Nel corso di tutta la relazione contrattuale, è assicurato un continuo monitoraggio, tramite verifiche periodiche sull'operato dei Responsabili esterni al fine di appurare il rispetto della normativa in materia di privacy e delle istruzioni impartite dal Titolare.
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 esterno anche coinvolgendo, qualora necessario, esperti in materia informatica.
Nel caso in cui emergessero criticità, è coinvolto il DPO, insieme alle funzioni aziendali interessate, per valutare interventi per la loro mitigazione. Qualora le criticità dovessero perdurare o fossero di un'entità tale da giustificare la cessazione del rapporto contrattuale, il Titolare interrompe la relazione contrattuale con il Responsabile esterno.
In caso di nomina di un nuovo Responsabile esterno o di modifica di Responsabili esterni esistenti, deve essere aggiornato conseguentemente anche il Registro dei trattamenti.
I dettagli operativi per la gestione dei Responsabili esterni sono descritti all'interno della specifica Procedura tempo per tempo aggiornata e pubblicata nel Documentale.

4) Gestione dei trattamenti

4.1) Condizioni di liceità del trattamento (Artt. 5 e 6 GDPR)

Il Titolare garantisce che i Dati personali 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).
In particolare, il Titolare adotta i presidi necessari ad assicurare che il trattamento di Dati personali sia effettuato solo ove ricorra 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 perseguire un legittimo interesse del titolare o di terzi, salvo che prevalgano gli interessi o i diritti e le libertà dell'interessato.

Nel dare avvio a una nuova tipologia di trattamento, il Titolare verifica con il coinvolgimento del DPO, che esso sia fondato su una delle fonti di liceità del trattamento di cui sopra.
Il Titolare fornisce agli Incaricati 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 mediante procedure che assicurino un agevole recupero di 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 possibile, i criteri utilizzati per determinare tale periodo.

4.2) Trattamento di dati di minori e di categorie particolari di dati personali (Artt. 8 e 9 GDPR)

Nel caso in cui il trattamento sia basato sul consenso e abbia ad oggetto Dati personali di minori, il Titolare assicura che il trattamento abbia luogo esclusivamente se tale consenso è 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 e il trattamento si basi sul consenso, il Titolare assicura che sia rilasciata un'informativa agli interessati e richiesto un consenso esplicito, nel rispetto delle Procedure interne, prima che il trattamento abbia inizio.

4.3) Cautele da adottare da parte dell'Incaricato

La permanenza di atti e documenti cartacei presso l'Incaricato deve essere limitata al tempo strettamente necessario per eseguire le operazioni di trattamento; al termine dell'attività la documentazione deve essere riposta nel rispettivo archivio.
Nel caso di documenti in output (si intendono come tali i documenti o i supporti contenenti Dati personali prodotti e rilasciati dalla struttura a soggetti esterni alla struttura stessa) è necessario all'atto della consegna o dell'invio, verificare che la persona che riceve il documento sia legittimata al ritiro e all'utilizzo.
L'Incaricato deve trattare qualunque prodotto dell'elaborazione di Dati personali, anche se non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, stampe elaborazioni temporanee ecc.) con le stesse cautele che sarebbero riservate alla versione definitiva.

4.4) Gestione del Registro dei trattamenti (Art. 30 GDPR)

Il Titolare gestisce la tenuta, l'aggiornamento e la conservazione del Registro dei trattamenti nel rispetto della normativa e della presente Policy.
Le funzioni aziendali coinvolgono il Referente privacy in fase di valutazione di attività che potrebbero comportare una modifica o istituzione di un trattamento e l'eventuale necessità di aggiornare il Registro dei trattamenti, tra cui a titolo esemplificativo:

- 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.

Il Registro dei trattamenti aggiornato deve essere reso disponibile a tutti gli Incaricati del Titolare secondo modalità atte ad assicurarne l'agevole consultazione.

5) Principi di protezione dei dati personali

5.1) Accountability (Art. 5 GDPR)

Per trattare i Dati personali in conformità con la normativa vigente e la presente Policy, il Titolare adotta misure tecniche, organizzative e di sicurezza adeguate, nonché adeguati meccanismi di controllo della costante conformità ti tali misure nel tempo e ne dispone il costante aggiornamento.
Il Titolare documenta le attività svolte per garantire che i trattamenti siano effettuati in conformità alla normativa applicabile e tiene tale documentazione a disposizione per eventuali accessi del Garante.

5.2) Privacy by design (Art. 25 GDPR)

Il Titolare assicura che tutte le applicazioni, servizi, prodotti ed attività che prevedono il trattamento di Dati personali siano 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 di modalità e mezzi del trattamento dei Dati personali, 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 a tutelare i diritti degli interessati.

5.3) Privacy by default (Art. 25 GDPR)

Il Titolare assicura che siano trattati, per impostazione predefinita, esclusivamente i Dati personali necessari per ogni specifica finalità del trattamento.

A tal fine, in fase di delineazione del trattamento, sono adottate le idonee misure tecniche e organizzative e sono valutati, in particolare, i seguenti elementi allo scopo di ridurre al minimo necessario l'impatto sul diritto alla protezione dei Dati personali rispetto alle finalità perseguite:

- quantità dei Dati personali da raccogliere;
- portata del trattamento;
- periodo di conservazione;
- numero di soggetti che ha accesso ai Dati personali.

I dettagli operativi per la gestione della **privacy by design e by default** sono descritti all'interno della specifica Procedura tempo per tempo aggiornata e pubblicata nel Documentale.

6) Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali (Artt. 44, 45 e 46 GDPR)

Il trasferimento di Dati personali all'esterno dell'Unione Europea può avvenire, in presenza di almeno una delle seguenti condizioni:

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

Il trasferimento di Dati personali verso un paese terzo o un'organizzazione internazionale sarà inoltre 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.

7) Diritti degli interessati

I diritti attribuiti dal GDPR agli interessati si dividono in due categorie: (i) i diritti che necessitano di una richiesta espressa dell'interessato; (ii) i diritti ai quali la normativa collega un obbligo del titolare in modo autonomo dalla ricezione di una previa richiesta dell'interessato.

7.1) I diritti subordinati a una richiesta espressa dell'interessato (Artt. 15-21 GDPR)

Il processo per la gestione dei diritti esercitati dagli interessati mediante espressa richiesta è riconducibile alle seguenti fasi principali:

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

Le modalità di gestione del predetto processo sono disciplinate nell'apposita Procedura tempo per tempo aggiornata e pubblicata nel Documentale.

I principali diritti che il GDPR garantisce all'interessato e che lo stesso può esercitare mediante richiesta sono i seguenti:

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'interessato 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 è 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 ai destinatari interessati prevista dall'articolo 19 GDPR.

7.2) I diritti non subordinati a una richiesta dell'interessato

Pur in assenza di richiesta da parte dell'interessato, il Titolare garantisce che allo stesso sia fornita idonea informativa al momento della raccolta dei suoi Dati personali presso lo stesso o, se i Dati non sono raccolti direttamente presso l'interessato, entro i seguenti termini:

- 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;
- nel caso in cui i Dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;
- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei Dati personali.

8) Misure di sicurezza (Art. 32 GDPR)

Il Titolare adotta le misure tecniche e organizzative opportune per 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, nonché del rischio di varia 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 o l'accesso non autorizzato a Dati personali, effettuati in modo accidentale o illegale. Qualora si verifichi una violazione di Dati personali, le misure tecniche e organizzative adottate devono comunque essere in grado di riconoscere e contrastare l'avvenuta violazione.

9) La valutazione d'impatto sulla protezione dei dati personali – DPIA (Art. 32 GDPR)

Nel caso in cui un determinato tipo di trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche (ad esempio 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, il Titolare, nella persona del Referente privacy, valuta la necessità o opportunità di effettuare una valutazione di impatto sulla protezione dei Dati personali in considerazione del rischio presentato dal trattamento e applicando la metodologia sviluppata e dettagliata nella Procedura tempo per tempo aggiornata e pubblicata nel Documentale.
Qualora la valutazione di impatto sulla protezione dei Dati personali 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.
Per i trattamenti già sottoposti a DPIA è prevista una revisione di tali valutazioni almeno ogni 3 anni.

10) Data breach (Artt. 33 e 34 GDPR)

Qualora si verifichi una violazione di Dati personali, le misure tecniche e organizzative adottate devono comunque essere in grado di riconoscere e contrastare l'avvenuta violazione.
Nel caso in cui si verifichi una violazione dei Dati personali che presenti un rischio per le libertà e i diritti degli interessati, il Titolare prevede una modalità immediata di reazione che permetta:

- 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;
- l'adozione delle misure necessarie ad attenuare gli effetti negativi della violazione.

Il Titolare tiene un registro delle violazioni e stabilisce procedure interne che disciplinano il suo aggiornamento al sussistere di ogni violazione, indifferentemente dal rischio presentato per i diritti e le libertà degli interessati e meccanismi di conservazione di tutte le comunicazioni riguardanti la violazione. In tale registro sono indicati tutti gli elementi richiesti dalla normativa applicabile, tra cui:

- le circostanze relative alla violazione;
- le conseguenze;
- le misure adottate per contrastarla e limitarne gli effetti;
- i Dati personali coinvolti; informazioni adeguate per permettere al Titolare di determinare le motivazioni per non aver effettuato la notifica, o averla effettuata in ritardo.

Il processo di gestione del Data Breach è dettagliato nella relativa Procedura tempo per tempo aggiornata e pubblicata nel Documentale.

11) Il sistema delle relazioni e dei flussi informativi

Sono definiti flussi informativi volti ad assicurare al DPO, agli Organi Aziendali ed alle funzioni di controllo la piena conoscenza e governabilità degli adempimenti in materia di protezione dei Dati personali.
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.
In particolare, sono garantiti almeno i seguenti flussi informativi:

- reporting verso gli Organi Aziendali: gli Organi Aziendali devono essere periodicamente 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) deve essere fornita una pronta informazione agli organi aziendali;
- reporting costante verso il DPO da parte del Referente privacy che rendiconta, almeno annualmente, i principali accadimenti in materia di protezione dei Dati personali relativi ai trattamenti di propria competenza;
- reporting costante verso il DPO da parte delle Funzioni Aziendali in merito ad ogni problematica riscontrata inerente il trattamento dei Dati personali.

I flussi informativi previsti ai sensi della presente Policy sono dettagliati nella relativa Procedura tempo per tempo aggiornata e pubblicata nel Documentale.

12) Allegati

La presente Policy è integrata dai documenti di seguito allegati:

- Allegato 1: Compiti del DPO
- Allegato 2: Compiti del Referente privacy

Policy in materia di protezione dei dati personali - Allegato 1

COMPITI DEL DPO

Il DPO e la struttura organizzativa a suo supporto rappresentano la principale funzione di consultazione, consulenza, sorveglianza e controllo in materia di protezione dei dati personali.

In conformità al Regolamento, il DPO è incaricato almeno dei seguenti compiti:

- **verificare nel continuo il rispetto della normativa** interna ed esterna in materia di protezione dei dati personali da parte delle unità organizzative del Titolare, mediante richiesta di documenti e/o accesso a tutte le banche dati contenenti informazioni utili all'espletamento dei propri compiti;
- **informare e fornire consulenza** al Titolare, nonché ai relativi incaricati del trattamento in merito agli obblighi derivanti dal Regolamento nonché dall'ulteriore normativa in materia di protezione dei dati personali;
- **fornire supporto e pareri** agli organi aziendali e agli incaricati del trattamento in merito all'interpretazione della normativa interna ed esterna in materia di protezione dei dati personali e alle corrette modalità di trattamento dei dati personali;
- **sorvegliare l'osservanza** del Regolamento e dell'ulteriore normativa interna o esterna in materia di protezione dei dati personali nonché delle politiche del Titolare o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- **collaborare** con il Titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;
- **cooperare con il Garante;**
- **monitorare l'evoluzione della normativa** e informare il Titolare in merito alla necessità di aggiornamenti della documentazione privacy e della normativa interna che si rendano necessari alla luce di tali evoluzioni normative;
- **raccogliere** dalle singole unità organizzative competenti **le segnalazioni** in merito alla necessità di aggiornamento della normativa interna;
- **proporre al Consiglio di Amministrazione** l'aggiornamento della normativa interna in materia di protezione dei dati personali alla luce del complessivo livello di conformità alla normativa tempo per tempo applicabile in materia;
- **coordinare e gestire i flussi informativi** in ambito privacy all'interno della struttura organizzativa del Titolare;
- **fungere da punto di contatto** con gli interessati e il Garante per questioni connesse al trattamento di dati personali, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento dei dati personali, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Policy in materia di protezione dei dati personali - Allegato 2

COMPITI DEL REFERENTE PRIVACY

Al Referente Privacy sono attribuite almeno le seguenti mansioni:

- esaminare gli aggiornamenti della normativa segnalati dal DPO;
- ricevere qualsiasi richiesta di consulenza da parte degli incaricati e del Titolare e, a seconda della complessità del quesito, (i) trasmetterla immediatamente al DPO, o (ii) rispondere direttamente;
- coadiuvare le funzioni competenti nella gestione dei diritti degli interessati qualora una richiesta presenti alcune problematiche e/o difficoltà che non richiedono l'intervento del DPO;
- sovrintendere il processo di selezione e nomina dei responsabili esterni e informare il DPO sullo svolgimento della procedura;
- coadiuvare il DPO nello svolgimento della valutazione di impatto sulla protezione dei dati DPIA;
- organizzare corsi di formazione in ambito privacy in linea con il piano approvato dal DPO;
- curare l'implementazione della documentazione e della normativa interna in materia di privacy;
- partecipare attivamente allo svolgimento delle analisi di privacy by design assicurando il rispetto della metodologia predisposta dal DPO, aggiornare costantemente il DPO e coinvolgerlo qualora risulti necessario;
- aggiornare il Registro dei trattamenti del Titolare, assicurando che siano sempre indicate informazioni complete e aggiornate;
- effettuare verifiche periodiche con report documentati presso i Responsabili esterni del Titolare, eventualmente avvalendosi delle risultanze delle Funzioni di Controllo e informare il DPO sugli esiti delle verifiche. Nel caso in cui il processo di verifica evidenzi una criticità, ivi inclusa una qualsiasi forma di inadempimento da parte del fornitore, coinvolgere immediatamente il DPO;
- gestire e aggiornare l'elenco dei responsabili esterni, assicurando che siano sempre indicati tutti i Responsabili esterni nominati;
- gestire e aggiornare l'elenco dei responsabili interni / amministratori, assicurando che siano sempre indicati tutti i soggetti nominati;
- ricevere ed eseguire ogni comunicazione del DPO, ivi inclusa la trasmissione delle istruzioni del DPO alle funzioni coinvolte;
- ricevere ogni segnalazione da parte del personale del Titolare su problematiche e criticità riscontrate in materia di protezione dei dati personali e informare prontamente il DPO;
- partecipare ad incontri periodici con il DPO;
- ricevere ogni segnalazione relativa alla violazione di dati personali relativa al Titolare e informare prontamente il DPO indicando, ove conosciuta, l'origine della violazione;
- coinvolgere il DPO qualora la gestione di una richiesta da parte di un interessato presenti particolari problematiche e/o l'interessato abbia richiesto il diretto intervento del DPO;
- trasmettere al DPO qualsiasi comunicazione o richiesta del Garante, e informarlo sull'eventuale volontà del Titolare e/o di una delle funzioni aziendali di contattare il Garante per qualsivoglia motivo;
- redigere un report annuale indirizzato al DPO e al Consiglio di Amministrazione del Titolare riguardante le attività svolte;
- assicurare che tutto il personale che tratta dati personali sia stato appositamente nominato incaricato del trattamento.