Policy in materia di protezione dei dati personali

Finalità del documento

Il presente documento si prefigge lo scopo di rappresentare come Banca Monte dei Paschi di Siena S.p.A. (nel prosieguo "Banca MPS"), in qualità di Titolare del trattamento, applica la propria politica di tutela della privacy attraverso il seguente approccio metodologico:

- presidio operativo e di controllo della privacy da concretizzare all'interno della Funzione Compliance, finalizzato a garantire: (i) rispetto dei principi in materia di tutela dei dati personali fin dalla fase di ideazione dei progetti o di utilizzo delle tecnologie; (ii) rispetto dei diritti esercitati dagli interessati; (iii) attuazione del Registro dei Trattamenti; (iv) gestione degli eventi di *Data breach*;
- ruoli e responsabilità in Banca MPS;
- flussi informativi in materia di privacy;
- programmazione e rendicontazione delle attività e dei controlli svolti in materia di tutela dei dati personali;
- formazione e responsabilizzazione dei dipendenti nelle attività di trattamento dei dati personali.

Il modello di gestione della privacy adottato dalle altre società del Gruppo è conformato al descritto approccio metodologico e tratta gli specifici ambiti inerenti alla materia secondo i processi definiti.

Principali contenuti Normativi

La normativa in materia di protezione dei dati personali è costituita da:

- il Regolamento Europeo in materia di Protezione dei Dati n. 2016/679, nel prosieguo Regolamento o GDPR, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (che abroga la Direttiva 95/46/CE);
- Decreto Legislativo 30.06.2003 n. 196 modificato dal Decreto Legislativo n. 101 del 10 agosto 2018 recante disposizioni per l'adeguamento dell'ordinamento nazionale al GDPR;
- principali norme esterne, nazionali ed europee, di riferimento (Leggi, Linee Guida e Provvedimenti pronunciati dal Garante per la protezione dei dati personali, pareri, Opinion del Comitato Europeo per la protezione dei dati (EDPB) stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione dei dati; protegge, inoltre, i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

Termini e Definizioni

Si illustrano i principali termini utilizzati nel Regolamento e nei principali Provvedimenti del Garante Privacy che assumono rilevanza in relazione all'operatività della Banca

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.
Trattamento	Qualunque operazione o insieme di operazioni che hanno per oggetto dati personali, effettuata anche senza l'ausilio di mezzi elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca di dati.
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 […].
Responsabile del trattamento	La persona fisica, la persona giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Registro dei trattamenti	Documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del GDPR) relative alle operazioni di trattamento svolte dal titolare e/o dal responsabile del trattamento. Costituisce uno dei principali elementi di accountability, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.
Accountability	Che tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. Inoltre, se ciò è proporzionato rispetto alle attività di trattamento, le predette misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

Privacy by design	Ha lo scopo di garantire l'esistenza di un corretto livello di privacy e protezione dei dati personali fin dalla fase di progettazione (design) di qualunque sistema, servizio, prodotto o processo, così come durante il loro ciclo di vita. In altre parole, il principio di "privacy by design" punta a garantire un corretto livello di protezione dei dati in tutte le attività di trattamento ed attuazioni effettuate all'interno di una organizzazione.
Privacy by default	Il principio della "privacy by default" prevede che il titolare individui, prima di iniziare il trattamento dei dati, quali dati personali sono strettamente necessari, per la finalità specifica per cui sono stati acquisiti, ai fini di proteggere la riservatezza dei dati personali.
Violazione di dati (*data breach*)	La 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.
Dati relativi alla salute	Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

1. Politica del trattamento dati in Banca MPS

1.2 Principi applicabili al trattamento dei dati

Nel trattamento dei dati personali riferiti a diverse categorie di soggetti interessati (es. clienti, *prospect* dipendenti, fornitori) Banca MPS applica i seguenti principi:

1. **liceità, correttezza e trasparenza**: (art. 5, comma 1, lettera a), per cui i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
2. **limitazione della finalità**: (articolo. 5, comma 1, lettera b), per cui i dati devono essere raccolti e registrati per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità;
3. **minimizzazione dei dati**: (art. 5, comma 1, lettera c), per cui i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **esattezza**: (art. 5, comma 1, lettera d), per cui i dati personali sono esatti e, se necessario aggiornati; inoltre devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
5. **limitazione della conservazione** (c.d. *data retention*), (art. 5 comma 1, lettera e), per cui i dati devono essere 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;
6. **integrità e riservatezza**: (art 5, comma 1, lettera f), per cui i dati personali sono 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 accidentale;
7. **privacy by design e privacy by default**: gli aspetti in materia di protezione dei dati personali devono essere considerati fin dalle fasi di progettazione, implementazione e configurazione di tutte le tecnologie utilizzate per le operazioni di trattamento. MPS deve trattare, di default, solamente quei dati che siano necessari al perseguimento delle finalità del trattamento;
8. **responsabilizzazione (c.d. accountability)**: la Banca è competente per l'osservanza dei suddetti principi e deve essere in grado di dimostrarlo.

1.3 Liceità del trattamento

Banca MPS effettua il trattamento di dati personali applicando le seguenti condizioni, in ragione dello specifico contesto del trattamento:

- Esecuzione contratto o di specifiche richieste da parte dell'interessato;
- obbligo legale cui è soggetta Banca MPS;
- esplicito consenso dell'interessato;
- salvaguardia di interessi vitali del soggetto interessato;
- perseguimento di un legittimo interesse.

1.4 Informativa sul trattamento

L'articolo 13 del GDPR prevede che il Titolare del trattamento informi previamente l'interessato oralmente o per iscritto, all'atto della raccolta dei suoi dati personali, circa il trattamento a cui gli stessi dati saranno sottoposti. In particolare, l'informativa deve contenere le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) in caso di trattamento per legittimo interesse, l'indicazione dei legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso di trasferimenti verso un paese terzo o un'organizzazione internazionale il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

In aggiunta alle informazioni sopra citate il titolare del trattamento fornisce all'interessato ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente (es. il periodo di conservazione dei dati, i diritti del soggetto interessato, ecc.).
Banca MPS ha predisposto numerose informative in relazione allo specifico contesto di trattamento dei dati, alcune delle quali sono presenti nell'apposita sezione del proprio istituzionale. In linea generale, per l'apertura di rapporti bancari o per l'esecuzione di operazioni occasionali che richiedono l'identificazione e il censimento del soggetto, all'atto della raccolta dei suoi dati viene fornita l'informativa privacy generale.

1.5 Richiesta del consenso

In Banca MPS, il consenso viene raccolto con riferimento:
a) al trattamento di categorie particolari di dati.
b) Appartengono a questa categoria quei dati personali atti a rivelare l'origine razziale ed etnica dell'interessato, nonché le sue convinzioni religiose, politiche, sindacali, l'adesione a partiti o sindacati, lo stato di salute, la vita sessuale ed i dati genetici e biometrici intesi a identificare in modo univoco una persona fisica;
c) alle finalità commerciali effettuate da Banca MPS.
d) Nel modulo di informativa riferito alle persone fisiche adottato dalla Banca sono previste quattro tipologie di trattamenti nei cui confronti l'interessato è libero di manifestare il consenso o il diniego.

Essi riguardano:
1) il trattamento di dati personali ai fini di informazione commerciale, ricerche di mercato, rilevazione del grado di soddisfazione sulla qualità dei servizi resi, invio di newsletter, inviti ad eventi, concorsi o iniziative a premi organizzati dalla Banca, offerte dirette di prodotti o servizi della Banca;
2) il trattamento di dati ai fini di informazione commerciale, ricerche di mercato, rilevazione del grado di soddisfazione sulla qualità dei servizi resi, invio di newsletter, inviti ad eventi, concorsi o iniziative a premi organizzati da Banca MPS, offerte dirette di prodotti o servizi di società terze;
3) la comunicazione a società terze ai fini di informazione commerciale, ricerche di mercato, invio di newsletter, inviti ad eventi, concorsi o iniziative a premi organizzati da Banca MPS, offerte dirette di loro prodotti o servizi;
4) il trattamento finalizzato all'analisi dei dati relativi ai rapporti e ai comportamenti dei clienti per l'individuazione e lo studio di loro profili di interesse o di preferenza riguardo ai servizi e prodotti della Banca, effettuati mediante elaborazioni statistiche in forma elettronica (per età, sesso, titolo di studio professionale, aree geografiche, frequenza ed importo delle transazioni con eventuale attribuzione anche di giudizi sintetici o punteggi), anche mediante aggregazione di dati personali.

Banca MPS ha adottato anche un modulo di informativa riferito alle **persone giuridiche** ove sono presenti le seguenti quattro tipologie di trattamenti nei cui confronti la società può manifestare il consenso o il diniego:

1) la comunicazione dei dati della società a soggetti terzi che effettuano attività di rilevazione della qualità dei servizi erogati;
2) il trattamento di dati personali ai fini di informazione commerciale, ricerche di mercato, rilevazione del grado di soddisfazione sulla qualità dei servizi resi, invio di newsletter, inviti ad eventi, concorsi o iniziative a premi organizzati dalla Banca, offerte dirette di prodotti o servizi di Banca MPS;
3) il trattamento, di dati ai fini di informazione commerciale, ricerche di mercato, rilevazione del grado di soddisfazione sulla qualità dei servizi resi, invio di newsletter, inviti ad eventi, concorsi o iniziative a premi organizzati da Banca MPS, offerte dirette di prodotti o servizi di società terze;
4) la comunicazione a società terze ai fini di informazione commerciale, ricerche di mercato, invio di newsletter, inviti ad eventi, concorsi o iniziative a premi organizzati dalla Banca, offerte dirette di loro prodotti o servizi.

1.6 Legittimo interesse

Banca MPS effettua alcuni trattamenti il cui presupposto di legittimità è stato identificato nel legittimo interesse del Titolare; di seguito se ne riportano alcuni:

1) valutazione dell'affidabilità e merito di credito (Rating interno del cliente e Credit Scoring), ottenuti consultando anche alcune banche dati esterne (in particolare i sistemi di informazione creditizia, c.d. SIC);
2) analisi volte a prevedere e prevenire eventuali irregolarità ed inadempienze nei pagamenti, o procedere al recupero del credito;
3) gestione di eventuali reclami e/o controversie di qualsiasi natura e in qualsiasi sede e grado, sia giudiziale che stragiudiziale;
4) prevenzione delle frodi;
5) analisi dei dati relativi ai rapporti bancari per l'individuazione e lo studio di servizi/ prodotti offerti o intermediati da Banca MPS di potenziale interesse, preferenza, probabilità di acquisto o, se già posseduti, di abbandono. Ciò, allo scopo di offrire prodotti/servizi specificamente individuati al fine di meglio indirizzare la propria offerta per rispondere più adeguatamente alle esigenze attuali e future della clientela. Tale trattamento prevede l'utilizzo di dati (es. prodotti posseduti, andamento dei rapporti, residenza, età) provenienti da varie fonti (interne o esterne alla Banca) per dedurre probabilità di comportamento di un soggetto, in base alle qualità o comportamenti di altre persone che sembrano statisticamente simili.

Per i trattamenti basati sul legittimo interesse Banca MPS, al fine di valutare se l'interesse legittimo del titolare prevalga o meno sugli interessi e i diritti dei clienti interessati, prima di iniziare il trattamento conduce un adeguato e documentato test comparativo (LIA - *Legitimate Interest Assessment*).

1.7 Trasferimento di dati all'estero

Per talune attività Banca MPS utilizza soggetti di fiducia - operanti talvolta anche al di fuori dell'Unione Europea - che svolgono, per conto della stessa, compiti di natura tecnica, organizzativa o gestionale. In tal caso, il trasferimento dei dati avviene sulla base delle ipotesi previste dalla vigente normativa (capo V del GDPR -

Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), tra cui l'applicazione di clausole contrattuali standard definite dalla Commissione Europea per i trasferimenti verso società terze o la verifica della presenza di un giudizio di adeguatezza del sistema di protezione dei dati personali del paese importatore.
Come riportato nel documento *Final Recommendations* dello *European Data Protection Board* (EDPB - *Final Recommendations*), adottato il 18 giugno 2021, prima di procedere al trasferimento dei dati occorre valutare se le leggi e le prassi del paese terzo di destinazione applicabili al trattamento dei dati personali da parte dell'importatore di dati potrebbero impedire a quest'ultimo di rispettare le clausole.
Per effettuare tale valutazione, Banca MPS conduce una valutazione di impatto del trasferimento dei dati Extra-UE (TIA - *Transfer Impact Assessment)* mediante la compilazione di un apposito documento sull'adeguatezza delle misure di salvaguardia per il trasferimento di dati verso paesi terzi che non sono presenti nella white list della Commissione UE.

1.8 Esercizio dei diritti previsti dall'interessato

Il GDPR riconosce all'interessato, quale legittimo "proprietario" dei dati, l'esercizio di alcuni diritti in relazione ai propri dati raccolti o comunque trattati dal titolare.

Più precisamente, agli articoli da 15 a 22, il GDPR elenca quali sono i diritti riconosciuti all'interessato:

- ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e quindi di venire a conoscenza della loro origine, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- ottenere gli estremi identificativi del titolare e dei responsabili del trattamento, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza;
- conoscere il periodo di conservazione dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- ottenere la rettifica, l'integrazione dei dati, nonché la cancellazione e la limitazione del trattamento;
- ottenere i dati personali che lo riguardano in un formato strutturato, di uso comune e leggibile da dispositivo automatico forniti dal titolare del trattamento ad un altro titolare senza impedimenti da parte del titolare che li ha forniti;
- Inoltre, l'interessato ha il diritto:
- di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali ancorché pertinenti allo scopo della raccolta;
- di opporsi, in tutto o in parte, al trattamento dei dati personali che lo riguardano ai fini di invio di materiale pubblicitario, o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale;
- proporre reclamo al Garante Privacy;
- conoscere l'esistenza di un processo decisionale automatizzato compresa la profilazione con l'indicazione della logica utilizzata, nonché le conseguenze previste per tale trattamento;
- essere informato dell'esistenza di garanzie adeguate ai sensi dell'art. 46 del Regolamento qualora i dati personali siano trasferiti ad un paese terzo.

Banca MPS gestisce le istanze della specie per il tramite dello Staff DPO che procede alla loro lavorazione ed evasione nei termini previsti dalla vigente normativa, ovvero entro un mese dal suo ricevimento, prorogabile a due mesi se le operazioni necessarie per un integrale riscontro sono di particolare complessità ovvero ricorre altro giustificato motivo).

1.9 Registro dei trattamenti e DPIA

Il Registro dei Trattamenti, introdotto dal GDPR, è un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del GDPR) relative alle operazioni di trattamento svolte dal titolare e/o dal responsabile del trattamento. Costituisce uno dei principali elementi di accountability, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.
Il Registro ha lo scopo di garantire l'applicazione del modello risk-based nella gestione della protezione dei dati personali e costituisce uno degli strumenti di controllo per i relativi adempimenti.

Banca MPS si è dotata di un applicativo informatico a cui possono accedere tutte le Funzioni interne nel cui contesto vi è trattamento di dati, in modo che possano mappare le attività di competenza. Quando una tipologia di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento stesso possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è necessario effettuare una DPIA. (Data Protection Impact Assessment) cioè una valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35 comma 1 del Regolamento), prima di procedere al trattamento. La DPIA, così come ciascun trattamento censito dalle singole Funzioni, viene valutata e approvata dal DPO.

1.10 Sicurezza del trattamento

Nel rispetto del principio di integrità e riservatezza dei dati previsto dall'art. 5 comma 1 lettera f) del GDPR, Banca Mps adotta misure organizzative e tecnologiche adeguate atte a garantire la riservatezza, l'integrità e la resilienza dei sistemi informatici.
Le misure di sicurezza soddisfano principalmente le esigenze di:

- **integrità**, che attiene all'esattezza ed alla completezza delle informazioni nonché alla protezione da manomissioni o da modifiche non autorizzate;
- **confidenzialità**, in base alla quale viene garantita l'accessibilità alle informazioni solo a soggetti precedentemente autorizzati;
- **disponibilità**, che implica la garanzia di accesso ai dati ed alle informazioni da parte del personale autorizzato ogniqualvolta ciò si renda necessario.

L'aspetto relativo alla sicurezza nel trattamento in Banca MPS viene garantito anche assegnando a ciascun dipendente, designato persona autorizzata al trattamento, un'utenza di accesso al Sistema Informativo della Banca, il cui profilo autorizzativo è in stretta il cui profilo autorizzativo è in stretta relazione al ruolo dallo stesso ricoperto, ai compiti affidati e all'entità operativa di appartenenza. L'accesso ai dati personali, sia informatici sia cartacei, da parte delle persone autorizzate al trattamento dei dati, è effettuato soltanto qualora la loro conoscenza sia strettamente necessaria per adempiere ai compiti assegnati e deve essere limitata ai soli dati effettivamente occorrenti ai fini dello svolgimento dei compiti loro assegnati.

1.11 Gestione degli eventi di *data breach*

Per violazione dei dati personali (***data breach***) si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni.
Il GDPR prescrive specifici adempimenti nel caso di una violazione di dati personali tra i quali:

1. la comunicazione al Garante della violazione dei dati, se il Titolare ritiene probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati. La notifica dovrà avvenire entro 72 ore dal momento in cui il titolare del trattamento ne è venuto a conoscenza;

2. la comunicazione all'interessato qualora dalla violazione possano derivare rischi per i diritti e le libertà degli interessati.

Banca MPS ha adottato processi interni per la gestione degli eventi che comportano una violazione sia IT che non IT, attribuendo specifiche responsabilità e compiti alle Funzioni interne della Banca ai fini della determinazione della gravità del rischio, Banca MPS adotta una griglia di valutazione per la definizione del rischio (limitato, trascurabile, rilevante, critico).

2. Ruoli e responsabilità in Banca MPS

Il Consiglio di Amministrazione di Banca MPS è responsabile della supervisione complessiva del sistema di gestione degli adempimenti relativi alla privacy; inoltre, approva le politiche ed il processo di gestione della privacy, fornendo gli indirizzi strategici in materia e impartendo le necessarie istruzioni affinché ne venga data concreta attuazione. Per Banca MPS Il Titolare del trattamento è il Consiglio di Amministrazione, che mantiene in capo a sé la responsabilità degli adempimenti privacy. Inoltre, in virtù di apposita delega, il Consiglio di Amministrazione ha autorizzato il Direttore Generale ad operare in materia di privacy, conferendogli i poteri necessari al fine di ottemperare alle disposizioni di legge, con facoltà di conferire deleghe e/o procure così come previsto dallo Statuto. A sua volta il Direttore Generale, in virtù di tali poteri, attribuisce le deleghe ad operare in materia di privacy ai Referenti Privacy, come di seguito specificato.

Considerata la dimensione della Banca e la varietà delle problematiche operative presenti in azienda, Banca MPS ha ritenuto opportuno individuare i Referenti Privacy, collocando tali punti di responsabilità nelle Strutture di Direzione Generale caratterizzate da contesti di trattamento di dati personali e/o da aspetti di particolare delicatezza e individuando i Referenti Privacy in funzione dell'incarico pro-tempore ricoperto, così da rispettare i requisiti richiesti di esperienza, capacità e affidabilità. Tale impostazione risulta coerente con le indicazioni del Garante Privacy, che ha stabilito che: "laddove sia compatibile con l'organizzazione o le attività dell'ente, vengano designate responsabili le persone in relazione alla funzione svolta (es. capo del personale, ecc.) in modo tale da creare automatismi a tutto vantaggio degli adempimenti burocratici" (cfr. comunicato stampa del Garante Privacy del 19 luglio 1999).

Considerata la dimensione della Banca e la varietà delle problematiche operative presenti in azienda, sono individuati più Referenti Privacy a cui sono attribuite **responsabilità comuni** a tutti (es. vigilare affinché il trattamento dei dati personali, sia dei dipendenti che della clientela, sia svolto in conformità ai principi definiti dall'art.5 del GDPR, far rispettare le misure di sicurezza adottate dalla Banca) e **specifiche**, in funzione dello specifico contesto operativo.

Il Data Protection Officer ("**DPO**") di Banca MPS è identificato nel Responsabile pro-tempore dello Staff DPO e Advisory ICT nell'ambito della Direzione Chief Compliance Executive. Il suo ruolo è deliberato dal Consiglio di Amministrazione della Capogruppo; anche altre società del Gruppo MontePaschi (es. Banca Widiba, MPS Fiduciaria), mediante apposito contratto e previa delibera del loro Consiglio di Amministrazione, hanno nominato quale DPO quello di Capogruppo.
Il DPO si avvale della collaborazione e del supporto dello Staff DPO che, nello svolgimento delle attività di sua competenza, esercita a livello di Gruppo la responsabilità attribuita dalla normativa GDPR (Regolamento UE 2016/679) per garantire la conformità agli obblighi previsti in materia di tutela dei dati personali attraverso le attività di consulenza ex-ante e *internal advisor* e la validazione di conformità della normativa interna, delle evoluzioni dei sistemi informatici e dei deliverable progettuali.

2.1 Data Protection Officer (DPO)

Ai sensi dell'art. 37 Banca MPS ha nomina il proprio DPO contattabile ai seguenti recapiti

- responsabileprotezionedeidati@postacert.gruppo.mps.it;
- responsabileprotezionedati@mps.it.

IL DPO costituisce un elemento chiave all'interno del sistema di *governance* dei dati personali e ad esso sono attribuiti dal GDPR compiti generali atti a facilitare e favorire l'osservanza della normativa attraverso strumenti di accountability; egli, inoltre, fungere da interfaccia tra i vari soggetti coinvolti (autorità di controllo, interessati e divisioni operative all'interno della struttura aziendale).

3. Flussi informativi in materia di privacy

Il Consiglio di Amministrazione di Banca MPS è destinatario di flussi informativi periodici, anche ricompresi nelle previste modalità di reporting (Relazioni, *Tableau de Bord* etc.) delle Funzioni di Controllo. Per espletare in modo integrato le attività assegnate, lo Staff DPO, oltre a disporre degli esiti delle attività di controllo svolte dalla Funzione controlli di conformità, riceve specifici flussi informativi da parte di ciascuna Direzione della Banca in relazione all'assolvimento degli adempimenti loro demandati in materia di privacy.
Per agevolare l'accesso alle informazioni rilevanti ai fini del presidio dei rischi in materia di tutela dei dati personali, tra gli Staff dei Chief di Direzione Generale della Banca ed il DPO, è stato istituito un momento di relazione e scambio da effettuarsi con periodicità semestrale.
Il confronto ha lo scopo di evidenziare criticità condivise e punti di attenzione nella quotidiana attività di gestione del tema Privacy, nonché stimolare e sviluppare nei Responsabili la consapevolezza sul tema.
Il DPO, inoltre, predispone una relazione annuale di riepilogo delle attività svolte, da sottoporre al Consiglio di Amministrazione della Banca. Tale report contiene le informazioni rilevanti sulle DPIA eseguite per Banca MPS, le principali evidenze rivenienti dai flussi informativi periodici inviati al DPO dalle diverse Direzioni della Banca, il riepilogo con le principali evidenze relative alle richieste di esercizio dei diritti (clienti e dipendenti), un prospetto riepilogativo relativo ai principali eventi di data breach, inclusi i casi invio della comunicazione all'Autorità garante e/o ai soggetti interessati.

4. Programmazione e rendicontazione delle attività e dei controlli svolti in materia di tutela dei dati personali

In coerenza con il modello di Compliance adottato la responsabilità di effettuare i controlli di secondo livello, mediante verifiche a distanza e/o in loco, sulle prescrizioni normative della disciplina relativa agli obblighi in materia di privacy è attribuita alla Funzione Controlli di Conformità.
In particolare, la Funzione Controlli di Conformità:

- pianifica ed effettua nel corso dell'anno i controlli a distanza e on-site, tenuto conto anche delle istanze avanzate dal DPO;
- qualora emergessero aspetti di non conformità nel comportamento dei dipendenti nell'ambito dell'assolvimento degli adempimenti loro demandati in materia di privacy effettua le comunicazioni alla Funzione Internal Audit e allo Staff DPO;
- effettua controlli di II livello sulla corretta esecuzione della DPIA;
- nell'ambito del reporting verso i vertici aziendali predisposto dal DPO, supporta il DPO relativamente agli esiti dei controlli di conformità in materia di privacy effettuati.

Circa gli applicativi adottati dalla Banca ai sensi del Provvedimento del Garante Privacy n. 192/2011 "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie", la Funzione Controlli di Conformità effettua i controlli sulla manutenzione ed aggiornamento delle regole, delle soglie e del perimetro delle applicazioni monitorate nell'ambito della generazione e gestione degli alert di Memento. L'esito dei controlli effettuati viene partecipato allo Staff DPO.

Formazione e responsabilizzazione dei dipendenti nelle attività di trattamento dei dati personali

Al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali, sono previsti interventi formativi sui dipendenti, ovvero altre iniziative atte a promuovere la cultura della protezione dati. Tali percorsi formativi riguardano non solo gli aspetti prettamente normativi (es. rispetto della normativa privacy, riservatezza dei dati, gestione di un data breach) ma anche quelli attinenti alla protezione dei dati sotto il profilo tecnologico, ad esempio relativamente al phishing o altre tecniche di truffe, corretto utilizzo delle dotazioni strumentali.
In relazione all'operatività di Banca MPS, considerato che:

1. l'esistenza di un rapporto di lavoro subordinato presuppone che il dipendente preposto al trattamento dei dati agisca su direttive comunque riferibili al Titolare che ne controlla necessariamente l'applicazione ed il rispetto tramite i "riporti" gerarchici previsti a livello aziendale;
2. la condizione di operare sotto la diretta autorità del titolare o del responsabile si realizza attraverso la stretta osservanza delle direttive aziendali (tra cui la normativa interna) in materia di trattamento dei dati, ivi comprese le istruzioni concernenti i profili della sicurezza e della riservatezza;
3. la designazione delle persone autorizzate al trattamento dei dati personali viene effettuata tramite le comunicazioni destinate ai lavoratori (lettera di assunzione, comunicazioni di trasferimento, Regolamenti) riguardanti l'assegnazione a determinate realtà operative comportanti, nello svolgimento dei relativi compiti, anche il trattamento di dati personali, comunque effettuato (manualmente e/o elettronicamente);
4. il ruolo in questione può essere ricoperto solo da persone fisiche alle quali vengono affidati compiti meramente esecutivi.

Le persone autorizzate al trattamento dei dati sono tutti i dipendenti che, in relazione alle attività svolte entrano in contatto e procedono a forme di trattamento dei dati personali a cui hanno accesso.
L'accesso ai dati personali, sia informatici sia cartacei, da parte delle persone autorizzate al trattamento dei dati, deve essere effettuato soltanto qualora la loro conoscenza sia strettamente necessaria per adempiere ai compiti assegnati e deve essere limitata ai soli dati effettivamente occorrenti ai fini dello svolgimento dei compiti loro assegnati. A tale proposito, come già indicato, ad ogni incaricato viene assegnata un'utenza di accesso al Sistema Informativo della Banca, il cui profilo autorizzativo è in stretta relazione al ruolo dallo stesso ricoperto, ai compiti affidati e all'entità operativa di appartenenza.