ASSOCIAZIONE DI MUTUA ASSISTENZA
fra il Personale della Banca Monte dei Paschi di Siena S.p.A.

ASSOCIAZIONE DI MUTUA ASSISTENZA FRA IL PERSONALE DELLA BANCA MONTE DEI PASCHI DI SIENA S.P.A., REGOLAMENTO IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO (UE) 679/2016

INDICE

1 - INFORMAZIONI PRELIMINARI

1.1 - Premessa

Il Regolamento costituisce il punto di riferimento delle attività finalizzate a perseguire il puntuale rispetto della normativa sul trattamento dei dati personali.
La normativa di riferimento, General Data Protection Regulation- Regolamento UE 2016/679, di seguito GDPR (entrata in vigore in data 25 maggio 2018), mira a garantire che il trattamento dei dati personali effettuato dal Titolare del trattamento si svolga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati, mediante l'adozione da parte del Titolare medesimo di regole e misure finalizzate ad evitare un trattamento illecito dei dati.
Le misure adottate dalla Società per garantire i suddetti diritti degli interessati consistono principalmente nella consegna dell'informativa all'interessato, nella raccolta dei consensi dallo stesso e nella traduzione di tale manifestazione di volontà nel sistema informatico. La Società svolge poi una serie di attività che vedono coinvolte unicamente le strutture interne e che hanno l'obiettivo di garantire la conformità della propria attività sul tema con la normativa sulla privacy.

2 - ASPETTI GENERALI

2.1 - Glossario

Il GDPR (**General Data Protection Regulation**- Regolamento UE 2016/679) mira a garantire gli obiettivi citati in premessa: ai fini di una più facile comprensione e di una corretta interpretazione delle prescrizioni legislative, si illustrano di seguito i termini principali citati nel presente documento, così come definiti ai sensi dell'art. 4 del GDPR.

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
Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Profilazione
Qualsiasi forma di trattamento automatizzato di dati personali consistenti 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.

Pseudominizzazione
Il trattamento di dati personali effettuato in modo tale che i dati non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che dette informazioni siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non possano essere ricondotti ad una persona fisica identificata o identificabile.

Titolare
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
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

Persone autorizzate al trattamento
Con tale definizione, che si può riscontrare in alcuni articoli del GDPR (ad esempio, art. 28), si identificano le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile. Si tratta, in sostanza, di coloro i quali nella precedente normativa italiana erano definiti "incaricati".

2.2 – I soggetti previsti dal codice privacy

2.2.1 – Il Titolare del trattamento

Titolare del trattamento (Titolare) è il soggetto che esercita, anche unitamente ad altro Titolare, il potere decisionale del tutto autonomo sulle finalità e modalità del trattamento dei dati personali (art. 4, punto 7 del GDPR).
L'art. 25 del GDPR riconosce al Titolare l'obbligo di mettere in atto misure tecniche e organizzative adeguate, volte a:
- attuare in modo efficace i principi di protezione dei dati;
- integrare, nel trattamento, le necessarie garanzie al fine di soddisfare i requisiti indicati nel GDPR e tutelare i diritti degli Interessati;
- garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

In sintesi, il GDPR mira a formalizzare la responsabilità, in capo al Titolare, di progettare e realizzare tutte le misure tecniche e organizzative adeguate ad assicurare l'applicazione dei principi di protezione dei dati, secondo quanto prescritto dal GDPR, sia nella sua fase iniziale (privacy by design), che in quella di prosecuzione del trattamento (privacy by default).
Peraltro, l'approccio proattivo, sistematico e continuo per la protezione dei dati attraverso l'adozione di misure di sicurezza appropriate che viene richiesto al Titolare, si basa anche sulla predisposizione di un'adeguata documentazione delle valutazioni che hanno portato a determinate scelte organizzative ed operative, in modo da poterla esibire a fronte di eventuali richieste dell'Autorità.
La volontà del Titolare si esplica, agli effetti della disciplina sulla protezione dei dati personali, tenendo conto delle ordinarie attribuzioni degli organi previsti dall'atto costitutivo, dallo Statuto e dalla normativa aziendale.
Associazione di Mutua Assistenza fra il personale della Banca Monte dei Paschi di Siena S.p.a. è Titolare del trattamento ed esercita il potere decisionale autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo sulla sicurezza, fermo restando il ruolo di consulenza della Banca MPS S.p.a., sulla base della delibera della Deputazione Amministratrice del 27.10.1977 fra Cassa di Mutua Assistenza fra il Personale del Monte dei Paschi di Siena S.c.r.l. e Banca MPS S.p.a.

2.2.2 - Il Responsabile del trattamento

Qualora un trattamento debba essere effettuato per conto del Titolare quest'ultimo ricorre al **Responsabile del trattamento (Responsabile)**, quale persona fisica o giuridica "preposta" al trattamento dei dati personali, individuandolo tra i soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate al fine di garantire che il trattamento soddisfi i requisiti previsti dal GDPR.
L'art. 28 del GDPR che disciplina tale ruolo stabilisce specifiche modalità per la nomina, ovvero prevede che i trattamenti da parte di un Responsabile siano disciplinati per iscritto tramite un contratto o altro atto giuridico, il quale preveda in particolare che il Responsabile:

- tratti i dati solo su istruzione documentata del Titolare anche in caso di trasferimento di dati verso un paese terzo;
- garantisca che le persone autorizzate al trattamento si siano impegnate alla riservatezza;
- adotti le misure di sicurezza previste dall'art. 32 del GDPR;
- assista il Titolare nelle richieste per l'esercizio dei diritti dell'interessato pervenute al Titolare;
- su indicazione del Titolare cancelli o restituisca i dati dopo che è terminata la prestazione dei servizi relativi al trattamento;
- metta a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nella nomina;

 prevede che qualora un Responsabile ricorra ad un altro Responsabile per l'esecuzione di specifiche attività di trattamento definite dal Titolare, possa nominarlo direttamente imponendogli, tramite un contratto o altro atto giuridico, gli stessi obblighi e le stesse istruzioni che ha ricevuto dal Titolare.

2.2.3 - Persone autorizzate al trattamento

Il GDPR non prevede, tra le definizioni di cui all'art. 4, la figura dell'incaricato del trattamento così come, invece, era espressamente definita dalla precedente normativa; tuttavia il GDPR fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del Regolamento), che possono essere assimilabili, per ruolo, agli incaricati.
Pertanto, le persone autorizzate al trattamento sono le persone fisiche che operano sotto la diretta autorità del Titolare o del Responsabile e che sono autorizzate ad eseguire operazioni di trattamento attenendosi alle istruzioni loro impartite. Atteso che il ruolo in questione può essere ricoperto solo da persone fisiche alle quali vengono affidati compiti meramente esecutivi, esse sono tutti i dipendenti che, in relazione alle mansioni svolte, procedono a forme di trattamento dei dati personali a cui hanno accesso: nel caso di Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a., i dipendenti distaccati da Banca MPS S.p.a..

2.2.4 - Incaricati esterni

Nelle aziende possono operare anche collaboratori esterni, quali ad esempio lavoratori a progetto, professionisti, stagisti, ecc., i quali, nell'ambito delle attività svolte, possono venire a conoscenza di dati personali. Anche in questi casi è indispensabile procedere alla loro designazione quali "Incaricati esterni" del trattamento e all'assegnazione delle relative istruzioni per il trattamento dei dati. La lettera di designazione sarà firmata dal Presidente della Associazione di Mutua Assistenza fra il personale della Banca Monte dei Paschi di Siena S.p.a.

2.2.5 - L'Interessato

La definizione di **interessato** è ricompresa all'interno dell'art. 4, comma 1 del GDPR ove viene trattata la definizione di "dato personale"; interessato è, pertanto, la persona fisica identificata o identificabile a cui si riferiscono i dati personali che possono essere oggetto di trattamento.

2.2.6 - Responsabile della Protezione dei Dati (Data Protection Officer - DPO)

L'art. 37, comma 1 del GDPR prevede che il Titolare e il Responsabile del trattamento provvedano a nominare il Responsabile della Protezione dei Dati o, utilizzando il termine inglese, Data Protection Officer (DPO) ogni qual volta, tra le altre fattispecie, il trattamento dei dati personali richiede il monitoraggio regolare e sistematico degli interessati su larga scala, tra cui rientrano senza dubbio anche quelli relativi ai dati dei clienti da parte di un OMC.
Il DPO, che può essere una persona fisica o giuridica interna o esterna all'azienda, ha il compito di assistere il Titolare e il Responsabile del trattamento nel controllo dell'effettivo funzionamento dei presidi posti in essere per garantire la protezione dei dati personali.

Al DPO, a cui deve essere riconosciuta una posizione di indipendenza e vigilanza sulla materia della privacy, vengono attribuiti i seguenti compiti:
a) informare e fornire consulenza al Titolare o al Responsabile del trattamento in merito agli obblighi derivanti dal GDPR o dalle disposizioni legislative interne o europee in materia di protezione dei dati personali;
b) monitorare l'osservanza del GDPR principalmente allo scopo di garantire la sicurezza del trattamento, sorvegliare sull'attribuzione delle responsabilità, sulla sensibilizzazione e la formazione del personale dipendente incaricato del trattamento;
c) fornire, su richiesta, pareri in merito alla valutazione d'impatto (Data Protection Impact Assessment, in seguito DPIA) e sorvegliarne lo svolgimento;
d) cooperare con le attività di controllo fungendo, tra le altre cose, da punto di contatto per questioni connesse al trattamento effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.
Infine, è un diritto degli interessati contattare il DPO per tutte le questioni relative al trattamento dei loro dati.
Il DPO viene designato tenendo conto che deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.
Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il Titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare.
Deve inoltre agire in piena indipendenza e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici. Il DPO deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.
Il DPO è, pertanto, una figura di vigilanza piuttosto che di garanzia, nel senso che al DPO non sono attribuite responsabilità personali in caso di inosservanza alle disposizioni del GDPR, le quali permangono in capo al Titolare e il Responsabile: dette figure, infatti, rimangono comunque responsabili per il rispetto della normativa sulla protezione dei dati personali ed alle stesse compete di dimostrare di aver messo in atto tutte le misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni presenti nel GDPR.

3 - ARTICOLAZIONE DELLE RESPONSABILITA' ALL'INTERNO DELLA SOCIETA'

3.1 – Aspetti generali

Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a. realizza la propria politica di tutela della privacy attraverso la distinzione e formalizzazione di ruoli e responsabilità a diversi livelli organizzativi, la responsabilizzazione dei dipendenti distaccati nelle attività di trattamento dei dati personali, la definizione di attività, compiti e flussi informativi, programmazione e risultati dell'attività privacy.
Per tutte le attività relative alla materia del trattamento dei dati personali Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a. si avvale della consulenza e del supporto della Banca MPS S.p.a., in particolare della sua Funzione Compliance, sulla base della delibera della Deputazione Amministratrice di Banca MPS del 27.10.1977

3.2 – Ruolo degli organi di vertice

3.2.1 – Organi con funzione di supervisione strategica

Il **Consiglio Direttivo dell'Ente** (di seguito C.D.) è responsabile della supervisione complessiva del sistema di gestione degli adempimenti relativi alla privacy. In particolare, il C.D. 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.
Il Consiglio Direttivo nomina il Data Protection Officer (DPO) esterno all'azienda, nominando quale DPO il medesimo nominativo individuato dalla Banca MPS in virtù della delibera della Deputazione Amministratrice del 27.10.1977 fra Banca MPS S.p.a. e Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a.. il C.D. è responsabile di assicurare un'efficace gestione dell'attività in materia privacy. In particolare:
- individua gli indirizzi strategici in materia;
- definisce le responsabilità delle strutture e delle funzioni della Società coinvolte nella gestione della privacy, assicurando la formalizzazione e la documentazione del processo;
- è responsabile del rispetto delle politiche e delle procedure in materia, accertandosi che in caso di violazioni vengano apportati i necessari rimedi.
La **Direzione**, in coerenza con le modeste dimensioni aziendali, il business ed il profilo di rischio che caratterizza l'azienda, assicura un'efficace gestione della privacy.
In particolare:
- attua gli indirizzi strategici definiti dal C.D.;
- concretizza i poteri attribuiti dal C.D.;
- definisce le responsabilità dei settori coinvolti nella gestione della privacy;
- è responsabile del rispetto delle politiche e delle procedure in materia, accertandosi che in caso di violazioni vengano apportati i necessari rimedi.

3.2.2 – Organo con funzioni di controllo

Il GDPR prevede, tra l'altro, che il DPO vigili sulla puntuale osservanza delle disposizioni. In tale ambito il Collegio Sindacale riceve dal DPO stesso la relazione in materia di privacy.

3.3 – Funzioni aziendali

Il **DPO** (esterno alla Società- vds. 3.2.1) svolge i seguenti compiti:
- conserva, controlla e revisiona periodicamente il registro dei trattamenti;
- può richiedere l'attivazione del processo DPIA;
- si confronta con il Garante nel caso in cui a seguito della DPIA il trattamento risulti ancora rischioso (consultazione preventiva secondo art. 36 GDPR);
- svolge reporting sulle DPIA effettuate in termini di esiti delle implementazioni necessarie a raggiungere un livello di sicurezza prefissato;
- informa il Garante in caso di *data breach* (violazione) sui dati personali;
- facilita/gestisce l'accesso, da parte dell'Autorità di Controllo, ai documenti e alle informazioni necessarie in caso di ispezioni/verifiche;
- sorveglia l'osservanza del GDPR e di altre disposizioni legislative relative alla protezione dei dati, compresa l'attribuzione delle responsabilità;
- considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;
- rendiconta periodicamente gli organi di vertice in relazione alle attività svolte.
Il DPO della Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a. è lo stesso della Banca MPS S.p.a.: esso peraltro intrattiene i rapporti con la Funzione Compliance della Banca MPS S.p.a.a cui può chiedere informazioni in merito ai trattamenti effettuati.

Al fine di sfruttare le sinergie presenti, il DPO è stato individuato dalla Banca MPS S.p.a. nel Responsabile pro-tempore del Servizio Compliance ICT, e a sua volta per tale ragione è stato indicato anche come DPO della Associazione di Mutua Assistenza fra il personale della Banca Monte dei Paschi di Siena S.p.a..
Pertanto la funzione Compliance della Banca MPS S.p.a. nell'ambito delle proprie prerogative opera in sinergia con il DPO della Associazione di Mutua Assistenza fra il personale della Banca Monte dei Paschi di Siena S.p.a. relativamente alla tematica privacy. Per lo svolgimento delle attività di competenza il DPO si avvale anche delle risorse del Servizio ICT Compliance della Banca MPS S.p.a..
La Banca MPS S.p.a. ha attribuito la responsabilità del governo operativo e dei controlli e della disciplina relativa agli obblighi in materia di privacy alla sua Funzione Compliance. Per espletare in modo integrato le attività assegnate, la Funzione Compliance, oltre a disporre degli esiti delle proprie attività di controllo, riceve relazioni periodiche dalla Funzione Revisione Interna della Banca MPS S.p.a., inerenti agli esiti della pertinente attività.
La **Funzione Business Owner**, che ha il compito dell'aggiornamento costante del registro dei trattamenti dei dati ai sensi del Regolamento (UE) 679/2016, è svolta all'interno della Associazione di Mutua Assistenza fra il personale della Banca Monte dei Paschi di Siena S.p.a. dalla Sezione Rapporti Operativi.

4 - ASPETTI GENERALI OPERATIVI

4.1 – Articolazioni e responsabilità

Come detto, il governo della materia e il presidio della conformità dei processi e delle attività appartiene, nella sua complessità, alla Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a. con il supporto della Funzione Compliance della Banca MPS S.p.a. e alla figura del DPO che costituiscono punto di riferimento del pieno rispetto e dell'osservanza delle disposizioni di cui al Regolamento (UE) 2016/679. Le strutture della Società sono tenute quindi ad attivarsi per le attività che abbiano attinenza con la materia, che non trovano risposte nella normativa ovvero che presentino particolari problematiche. Le disposizioni contenute nel presente documento costituiscono nel loro complesso le norme operative da osservare nell'espletamento di qualsiasi forma di trattamento di dati e pertanto, in relazione al loro ambito di attività, valgono per tutte le risorse umane (sia distaccati che volontari) della Società coinvolte nel trattamento dei dati.

4.2 - Nomina dei responsabili e delle persone esterne autorizzate al trattamento dei dati personali

Nell'espletamento della propria attività, le persone autorizzate al trattamento dei dati effettuano materialmente le operazioni di trattamento dei dati personali e operano sotto la diretta autorità del Titolare (art. 14 del Decreto). Il Titolare del trattamento è tenuto a designare per iscritto le persone autorizzate al trattamento dei dati con indicazione dei compiti assegnati e dei trattamenti consentiti.
Spettano alla Società le decisioni in ordine alle finalità e modalità dei trattamenti effettuati sia dal Responsabile che dalla persona autorizzata al trattamento dei dati personali. Conseguentemente, grava sulla Associazione di Mutua Assistenza fra il personale della Banca Monte dei Paschi di Siena S.p.a. l'obbligo di vigilare sui trattamenti in questione, anche sotto il profilo delle misure di sicurezza adottate o da adottare.
Dato che la Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a. si appoggia alla Banca MPS S.p.a. per molte delle sue attività, Banca che a sua volta utilizza il Consorzio Operativo Gruppo MPS S.p.a. con riferimento alla fornitura di servizi inerenti la gestione del sistema informatico aziendale e considerato poi che il programma gestionale della Associazione di Mutua Assistenza fra il personale della Banca Monte dei Paschi di Siena S.p.a. è fornito e amministrato dal Consorzio Operativo Gruppo MPS S.p.a., ricoprendo così entrambi il ruolo di Responsabili del trattamento. Intervenendo su ambiti informatici sensibili ai fini della tutela della privacy, devono rispettare le previsioni normative che regolano la materia e adottare le necessarie cautele e misure di protezione a salvaguardia delle utenze privilegiate di cui dispone e dei dati contenuti negli ambiti informatici resi accessibili grazie alle medesime.

Gli articoli 15-22 del Regolamento obbligano la Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a., in qualità di Titolare del trattamento, a fornire idoneo riscontro alle richieste di esercizio dei diritti avanzate dagli interessati ai dati personali che li riguardano. Tra questi devono essere annoverate, a titolo esemplificativo e non esaustivo, tutte le informazioni anagrafiche, le informazioni ai rapporti intrattenuti, le informazioni relative alle operazioni effettuate dagli interessati, ecc. In particolare, i diritti disciplinati dal Regolamento sono i seguenti:

Diritto di **accesso**: il diritto di ottenere, in un formato di uso comune, l'accesso ai dati personali e le relative modalità di trattamento in corso, in particolare le finalità, le categorie dei dati trattati, il periodo di conservazione, eventuali destinatari terzi a cui sono stati comunicati e l'eventuale esistenza di meccanismi di profilazione. Il diritto di accesso (art. 15 del Regolamento) così disciplinato deve essere distinto dal diritto di accesso alla documentazione bancaria previsto dall'articolo 119 del TUB. Quest'ultimo, infatti, diversamente dal diritto di accesso, riconosce al cliente, a colui che gli succede a qualunque titolo e a chi subentra nell'amministrazione dei suoi beni, il diritto di ottenere copia di atti o documenti bancari, sia che essi contengano dati personali relativi all'interessato, sia nel caso in cui contengano dati riferiti a terzi. Infatti tale diritto non prevede limitazioni rispetto all'estensibilità delle informazioni contenute nella documentazione richiesta nemmeno nelle forme di un parziale oscuramento delle informazioni stesse; il suo esercizio prevede il pagamento delle spese a carico del
cliente.

Diritto di **rettifica**: il diritto prevede la possibilità di rettifica/integrazione dei dati personali nel caso di ravviso di inesattezze da parte del Titolare;

Diritto alla **cancellazione** ("diritto **all'oblio**"): il diritto di «essere dimenticato» da parte del Titolare tramite la cancellazione dei dati personali senza ingiustificato ritardo, nei casi in cui, tra gli altri, non siano più necessari per le finalità previste dal trattamento oppure venga revocato il consenso;

Diritto di **limitazione** di trattamento: il diritto di ottenere la limitazione di dati personali trattati, nei casi in cui viene contestata l'esattezza dei dati, il trattamento è illecito o i dati trattati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

Diritto alla **portabilità** dei dati: il diritto di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivi automatici, i dati personali dal Titolare del trattamento e di trasmettere tali dati ad un altro Titolare del trattamento senza impedimenti da parte del Titolare di origine;

Diritto di **opposizione**: il diritto di opporsi, per motivi connessi alla situazione particolare dell'interessato o per finalità di marketing diretto, al trattamento dei dati personali, compresa la profilazione.

Per agevolare le richieste di esercizio dei diritti da parte dell'interessato, il Titolare può designare un Responsabile quale soggetto deputato ai riscontri agli interessati: data la struttura leggera della Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a., questo non succede nella Società.

Le richieste degli interessati che intendano avvalersi della facoltà di avere informazioni in ordine al trattamento, alla comunicazione dei propri dati personali o che intendano esercitare un diritto come sopra indicato, devono far pervenire alla Società una comunicazione mediante lettera raccomandata, telefax o posta elettronica.

L'evasione delle richieste deve essere effettuata entro un mese dalla data di ricezione, con possibilità di prorogare il termine di ulteriori due mesi, previa comunicazione in tal senso all'interessato, ove le operazioni per un integrale riscontro siano particolarmente difficoltose. L'istanza dell'esercizio dei diritti è gratuita, salva la previsione di un contributo spese in presenza di una richiesta da parte dell'interessato di riprodurre uno speciale supporto su cui i dati personali figurano. Nel caso in cui l'estrazione dei dati risulti particolarmente difficoltosa, è possibile fornire riscontro alla richiesta anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti, ancorché la disciplina di protezione dei dati non preveda l'obbligo per il Titolare del trattamento di esibire o allegare copia di ogni singolo documento. I dati possono essere comunicati al richiedente anche oralmente o offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione sia agevole. La comunicazione agli interessati non può riguardare dati personali relativi a terzi; pertanto, nel caso di consegna di copia di documentazione che li contenga, devono essere oscurati.

Ai sensi dell'art. 15 del Regolamento, "al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio". Ciò implica che, per quanto riguarda i dati non strutturati, sarà vietato mantenere dati personali della clientela salvati, per esempio, su cartelle e/o chiavette USB.
Il diritto di accesso ai dati personali, di cui all'art. 15 del Regolamento, così come gli altri diritti disciplinati negli artt. da 16 a 22 del Regolamento, riferiti a persone decedute possono essere esercitati ai sensi dell'art. 13 comma 23 del Decreto "da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione" legittimando i soggetti che si trovino in tali condizioni ad esercitare tale diritto in rapporto a dati personali (inclusi rapporti bancari e finanziari) riferiti al defunto.

4.3 - Consegna dell'informativa e raccolta del consenso – Soci

Il trattamento dei dati personali avviene previa dazione dell'informativa ex art. 13 del Regolamento ed acquisizione dei consensi in relazione ai diversi trattamenti effettuati dal Titolare. Si precisa che detto obbligo riguarda solo le persone fisiche, in quanto il D.L. n. 201/2011 (c.d. Decreto Salva Italia) convertito, con modificazioni, dalla L. n. 214/2001 ha limitato l'oggetto e l'ambito di applicabilità del Codice alle sole persone fisiche, escludendo le persone giuridiche, gli enti e le associazioni (art. 40, comma 2), seppur con le eccezioni riferite ai trattamenti effettuati per finalità di marketing con sistemi automatizzati (e-mail sms, chiamata senza operatore, ecc.), per i quali, anche nei confronti delle suddette categorie di soggetti, è necessario acquisire il preventivo consenso. Associazione di Mutua Assistenza fra il Personale della Banca Monte dei Paschi di Siena S.p.a. utilizza un solo modulo ("Informativa e consenso al trattamento dei dati personali"), modificato rispetto al passato secondo la nuova normativa GDPR, strutturato secondo le indicazioni in essa contenute: il modulo, al momento della presentazione della domanda da parte del Socio, indipendentemente dall'esito dell'istruttoria, viene fatto sottoscrivere e consegnato in copia al Socio.
In caso di cointestazioni, il consenso deve essere sottoscritto congiuntamente da tutte le singole persone fisiche della cointestazione.

5- VALUTAZIONE DI IMPATTO PRELIMINARE SULLA PROTEZIONE DEI DATI PERSONALI

Il GDPR abolisce l'istituto della notificazione del trattamento al Garante Privacy, il "prior checking". Essi sono stati sostituiti da verifiche ex post, cioè compiute successivamente alle determinazioni assunte autonomamente dal Titolare del trattamento. Come previsto dal GDPR, ogni qualvolta da un trattamento di dati personali possa derivare un rischio elevato per i diritti e le libertà delle persone a cui si riferiscono i dati, è necessario effettuare una valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment – DPIA) propedeutica al trattamento stesso. La DPIA deve pertanto essere effettuata ad ogni nuovo trattamento di dati o quando interviene una modifica sostanziale di un precedente trattamento effettuato dalla Società. Dall'esito della DPIA si evidenzia lo stato di sicurezza del trattamento e, successivamente a tale valutazione, il responsabile interno (Business Owner) procede ad aggiornare il registro dei trattamenti.
La DPIA effettua una valutazione preliminare che mira a valutare il **rischio inerente** per i diritti e le libertà delle persone fisiche derivanti dal nuovo o modificato trattamento dei dati personali o dalla revisione delle modalità di un trattamento esistente indipendentemente dall'esistenza di misure tecniche e organizzative di sicurezza e protezione poste a presidio. Lo scopo della valutazione preliminare della DPIA è quello di fornire al Business Owner le evidenze per capire se i trattamenti analizzati debbano essere soggetti alla valutazione di impatto.
Il livello di rischio inerente risultante dalla valutazione può assumere i seguenti livelli di rischio:
- **Critico** (*La valutazione di impatto sulla protezione dei dati - DPIA è sempre richiesta*);
- **Rilevante** (*La valutazione di impatto sulla protezione dei dati - DPIA può essere richiesta al DPO*);

- **Limitato** (*La valutazione di impatto sulla protezione dei dati - DPIA può essere richiesta dal DPO*)**;**
- **Trascurabile** (*La valutazione di impatto sulla protezione dei dati - DPIA può essere richiesta dal DPO*)**.**

La valutazione di impatto sulla protezione dei dati mira a evidenziare i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali e devono essere identificate le misure di sicurezza finalizzate a mitigare i rischi evidenziati all'interno della DPIA.
La valutazione di impatto dati personali viene eseguita quando il livello di rischio è "rilevante" o "critico".
Può essere consultato preliminarmente il Garante Privacy qualora si verifichino determinate casistiche e, in caso di consultazione al Garante Privacy, il DPO dovrà fornire specifiche informazioni ai sensi dell'art. 36 del GDPR. Lo stesso articolo stabilisce che "*l'autorità di controllo [n.d.r. Garante Privacy] fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al Titolare del trattamento e, ove applicabile, al responsabile del trattamento, prorogabile di sei settimane, tenendo conto della complessità del trattamento previsto*".

5.1 - Reporting

Il report DPIA è formalizzato per ogni processo DPIA completo, ovvero in tutti quei casi in cui l'esito della valutazione preliminare ha identificato un rischio inerente "critico" o "rilevante" e nel qual caso è stato ritenuto necessario procedere con la valutazione delle misure tecniche e organizzative di sicurezza e protezione poste per mitigare il rischio per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali. Il Report DPIA ha specifica struttura e fornisce informazioni definite.
I report DPIA vengono conservati presso l'ufficio del DPO. Il DPO predispone una relazione di sintesi su tutte le DPIA eseguite, da sottoporre al Consiglio di Amministrazione della Banca, con scadenza trimestrale se avvalorate.

6 - GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

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. Segnalatore di incidenti deve intendersi ogni struttura organizzativa aziendale che sia venuta a conoscenza di un fatto che possa costituire una potenziale data breach.
Ogni volta che si presenta una potenziale violazione di dati personali di natura non IT (es. ritrovamento in luogo incustodito di documenti cartacei che riportano dati personali, violazione di archivi in cui sono custoditi documenti cartacei riferiti a dati personali), si deve attivare la segnalazione, raccogliendo informazioni sull'incidente. E' opportuno cercare di discriminare se tale evento abbia generato un effettivo impatto sui dati personali.
In caso affermativo (anche in caso di potenziale violazione o di incidente avvenuto presso un fornitore) devono essere raccolte le informazioni associate rilevando la natura della violazione, la tipologia di dati, gli interessati coinvolti.
Una volta analizzata la potenziale violazione, si procede alla sua classificazione valutando il rischio associato di violazione dei diritti e alle libertà degli interessati.
Se viene accertato che trattasi di violazione dei dati personali con rischio rilevante o critico è necessario attivare la Notifica verso il Garante Privacy entro 72 ore dall'evento.
Una volta classificato l'evento come "major incident" connesso alla violazione di dati non IT, occorre effettuare le attività di analisi e diagnosi per fornire una soluzione alla violazione dei dati personali.
La principale finalità di questa fase è l'implementazione della soluzione identificata nella fase di diagnosi per la risoluzione della violazione. Lo scopo della fase della chiusura della violazione dei dati personali è definire le modalità di chiusura dell'incidente.

6.1 - Gestione della notifica all'autorità di controllo e agli interessati

Nel caso in cui durante la fase di classificazione si sia riscontrato un rischio per i diritti e le libertà dell'interessato è necessario gestire l'evento come "Major Incident". Dopo la notifica iniziale, il Titolare potrebbe aggiornare l'autorità di controllo nel caso in cui un approfondimento abbia rilevato che l'incidente di sicurezza sia stato efficacemente contenuto. Inoltre il DPO effettua verifiche sul registro delle violazioni al fine di verificare che gli adempimenti presenti nelle presenti linee guida siano rispettati.