MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Allegato B

ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI

In via preliminare, Le forniamo alcune informazioni generali sul GDPR. Tale normativa protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

- Per "*trattamento*" si intende qualunque operazione o complesso di operazioni, effettuate con o senza l'ausilio di processi automatizzati e applicate ai 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.
- Per "*dato personale*" si intende qualunque informazione relativa a persona fisica, identificata o identificabile ("*interessato*"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificativo, 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.

In relazione alla Sua nomina quale "*persona autorizzata al trattamento dei dati*", Le forniamo le istruzioni relative alla sicurezza e tutela dei dati personali che Le chiediamo di osservare.

1. AMBITO DELLA SUA NOMINA

La nomina è relativa al trattamento dei dati personali (riferiti a clienti, dipendenti o fornitori della Banca) a cui può avere accesso – con o senza l'ausilio di strumenti elettronici - nell'ambito delle mansioni che Le sono affidate. Il trattamento deve riguardare i soli dati necessari per lo svolgimento della Sua attività lavorativa, adottando la massima sicurezza e riservatezza delle informazioni di cui viene in possesso, considerando tutti i dati personali confidenziali e, di norma, soggetti al segreto bancario; inoltre, devono essere evitate attività o comportamenti che possano determinare eventuali rischi di perdita o distruzione anche accidentale dei dati trattati, di accesso non autorizzato, o di trattamento non consentito o non conforme ai fini per i quali i dati stessi sono stati raccolti.

2. PRINCIPI GENERALI DI COMPORTAMENTO

La "*persona autorizzata al trattamento*" si impegna a:

- operare con la massima attenzione e riservatezza in tutte le fasi del trattamento, astenendosi dall'eseguire operazioni per fini diversi dai compiti assegnati;
- trattare e custodire tutti i dati, indipendentemente dalla loro natura o dalle operazioni eseguite sui dati stessi, con diligenza, evitando azioni che possano renderli conosciuti a terzi non autorizzati;
- effettuare l'accesso ai sistemi informatici osservando le regole di sicurezza imposte dalla Banca e riportate nel seguente paragrafo sulle "**istruzioni di sicurezza**";
- attenersi alle indicazioni del tutor aziendale e fare riferimento al medesimo per qualsiasi esigenza di tipo organizzativo o in merito alle presenti istruzioni o, infine, per altre ragioni che dovessero sopraggiungere;

- astenersi dall'effettuare copie, di qualsiasi natura, concernenti i documenti interni aziendali o altro materiale contenente i dati personali per fini personali o estranei all'attività, evitando di portarli all'esterno del luogo di lavoro o di consegnarli o comunicarli a terzi non autorizzati;
- fornire al Responsabile interno del trattamento, a semplice richiesta e secondo le modalità indicate dal medesimo, tutte le informazioni relative all'attività svolta, al fine di consentire di svolgere efficacemente la prevista attività di controllo;
- prestare, in linea generale, la più ampia e completa collaborazione al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico ricevuto, nel rispetto della normativa vigente.

3. PRINCIPI DI COMPORTAMENTO IN MATERIA DI SICUREZZA LOGICA E FISICA

La presente sezione comprende le istruzioni operative generali relative a:

- Parola chiave per l'accesso ai dati;
- Antivirus e protezione da programmi pericolosi;
- Accesso ai soli dati necessari;
- Custodia di atti e documenti.

3.1. Parola chiave per l'accesso ai dati

Tutte le *"persone autorizzate al trattamento"* dispongono di una parola chiave personale per l'accesso ai dati. La parola chiave, necessaria per l'accesso ai dati, è obbligatoria sia per l'accesso agli elaboratori stand alone, sia per gli elaboratori connessi in rete, nonché per gli elaboratori che operano con la doppia modalità (stand alone e/o connessi in rete) e indipendentemente dalle caratteristiche della rete circa la connessione a reti di telecomunicazioni disponibili al pubblico.
La parola chiave (password) assegnata al momento del primo accesso al sistema deve essere immediatamente variata da ciascun soggetto. Essa, autodeterminata dai singoli soggetti, deve essere composta da 8 caratteri numerici e va variata frequentemente e comunque almeno una volta al mese.

Al fine di proteggere la segretezza delle password è necessario attenersi alle seguenti istruzioni:

- la password è strettamente personale: deve essere custodita con la massima cura e non va assolutamente comunicata ad alcuno, per nessun motivo, anche se richiesta;
- la prima assegnazione della password al nuovo utilizzatore è contestuale all'attribuzione della Userid da parte del Settore Gestione Utenti del Consorzio Operativo MPS;
- la password "di prima assegnazione" deve essere immediatamente cambiata dall'assegnatario, prima che lo stesso possa svolgere qualsiasi altra operazione. Al primo collegamento in assoluto con il sistema è richiesto il cambio della password iniziale;
- la password deve avere lunghezza di 8 caratteri;
- la nuova password deve essere creata nella maniera più casuale possibile, evitando l'utilizzo di password già usate in precedenza (le ultime 5 password) e di password facilmente individuabili (data di nascita, numeri telefonici, ecc.);
- il cambio della password deve essere confermato, ribattendo la stringa di caratteri una seconda volta per evitare equivoci;
- l'inserimento della password deve essere mascherato allo scopo di evitarne l'individuazione da parte di eventuali osservatori;

- successivamente alla prima assegnazione, la password rimane di esclusiva responsabilità e gestione dell'assegnatario, che può modificarla con modalità e tempi che ritiene opportuni e comunque almeno una volta al mese;
- è opportuno variare la password di frequente in modo da evitare la conoscenza da parte di altre persone. In particolare, è consigliabile cambiare la propria password ogniqualvolta si tema che possa essere stata individuata fortuitamente da qualcuno e con maggiore frequenza in occasione dello svolgimento di lavori particolarmente riservati;
- la generazione di una nuova password da parte dell'assegnatario implica necessariamente la titolarità e la validità della precedente;
- evitare di scrivere la propria password in luoghi facilmente accessibili, ad esempio sul terminale, sul manuale delle istruzioni, ecc. Nel caso si voglia conservarne traccia scritta, per propria memoria, essa deve essere conservata con cura ed in luogo chiuso, e con modalità che non ne consentano una facile interpretazione;
- evitare di immettere la propria password quando si è osservati;
- in caso di necessità di breve allontanamento dal proprio posto di lavoro è necessario bloccare il posto di lavoro allo scopo di evitare che altre persone accedano ai dati e possano eseguire operazioni utilizzando il codice identificativo e la parola chiave già attivati.

3.2 Antivirus e protezione da programmi pericolosi

Su tutti i computer dell'azienda è attivo un antivirus. Tale modulo intercetta tutte le operazioni eseguite dall'utente eseguendo una scansione da virus ogni volta che un file viene aperto, copiato, creato o rinominato, oltre ai controlli sui floppy disk inseriti, nonché all'accensione e allo spegnimento del computer. Ciò permette di isolare i virus riconosciuti prima che possano diffondersi. In ogni caso, è vietato l'uso di software che non sia stato preventivamente autorizzato e controllato.
Il Consorzio Operativo MPS, cui è affidata la gestione del sistema informativo aziendale, provvede ad aggiornare periodicamente i programmi antivirus.

Si ricorda, inoltre, che:

- nei locali della Banca non è ammessa la presenza né l'utilizzo di apparecchi *hardware* che non siano di proprietà della Banca stesso e per i quali non sia stata autorizzata la sussistenza;
- sulle apparecchiature informatiche della Banca non devono essere installati, neppure temporaneamente, *software* e/o programmi non gestiti e/o autorizzati dalla Banca stessa. È fatto, altresì, divieto di importare programmi da Internet se non per uso professionale attinente alle funzioni svolte e previa autorizzazione della Banca;
- è consentito l'accesso a siti Internet esclusivamente per ragioni professionali, quindi l'utilizzo dovrà riguardare esclusivamente finalità professionali;
- le caselle di posta elettronica sono messe a disposizione dall'azienda per usi esclusivamente professionali; l'invio di mailing list generalizzato o a gruppi di soggetti è consentito solo al personale autorizzato;
- i virus informatici, diffondendosi tramite *internet*, messaggi di posta elettronica o attraverso l'uso di *supporti magnetici* non distribuiti dall'azienda, possono alterare o addirittura distruggere i *file*;

- non devono pertanto essere utilizzati supporti magnetici (chiavette usb, dischi esterni, *compact disk, altro)* di provenienza sconosciuta, ovvero già utilizzati su altri elaboratori che hanno manifestato un cattivo funzionamento. Prima dell'utilizzo, è necessario assicurarsi che i supporti riutilizzati per la memorizzazione dei dati siano stati preventivamente verificati con software antivirus per evitare eventuali infezioni da virus informatici;
- è necessario controllare che il computer con cui si lavora sia dotato di software antivirus (Viruscan) e che esso sia aggiornato (la raccomandazione vale, in particolare, nel caso in cui vengano utilizzati elaboratori che non dispongono della piattaforma S.I.P., per i quali l'aggiornamento del programma antivirus viene effettuato manualmente);
- se si opera su elaboratori *stand-alone* è opportuno fare una copia di backup dei dati archiviati su supporti magnetici esterni (chiavette usb, hard disk esterni, *floppy o compact disk),* da conservare in luogo protetto (armadio chiuso a chiave, cassaforte).

3.3 Accesso ai soli dati necessari

Durante lo svolgimento di trattamenti di dati personali di qualunque natura registrati su carta o altri mezzi non magnetici utilizzabili da computer, *"le persone autorizzate al trattamento"* devono operare in modo da svolgere operazioni di trattamento solo su quei dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti previsti per le specifiche attività attribuite alla funzione ricoperta. È pertanto vietata ogni forma di trattamento di dati personali non pertinente con le operazioni previste per la propria posizione e mansione.
L'accesso agli archivi contenenti atti e documenti di dati personali di qualunque natura è riservato alle sole persone incaricate ed autorizzate a potervi accedere.

3.4 Custodia atti e documenti

Gli atti e i documenti, di qualunque natura, devono essere trattati con diligenza, custoditi e conservati in maniera che le persone prive di autorizzazione non possano venirne a conoscenza. Pertanto, tutta la documentazione riportante dati personali che non serve per lo svolgimento del lavoro deve essere riposta in armadi o in cassetti. Qualora ci si debba assentare dalla stanza in cui si lavora, la documentazione riportante dati personali non deve essere lasciata incustodita, ma deve essere riposta in armadi o cassetti per evitare che terzi, anche accidentalmente, possano venirne a conoscenza.
Nessun dato personale, su supporto magnetico, digitale o cartaceo, potrà comunque essere lasciato incustodito o posto al di fuori del luogo in cui l'incaricato svolge la propria attività né, fatti salvi i casi previsti e/o autorizzati, potrà in alcun caso essere trasferito su sistemi non di proprietà della Banca. In caso di mal funzionamenti dell'hardware dei personal computer che richiedono interventi di manutenzione, riparazione o sostituzione di dischi contenenti dati personali, o la consegna all'esterno dei dischi fissi o dell'intero PC o PC portatili, la richiesta di manutenzione o di riparazione dovrà essere preventivamente autorizzata seguendo le regole aziendali in vigore. In ogni caso, tutto il materiale cartaceo non potrà essere lasciato incustodito sulle scrivanie, sui banconi, ripiani o altro e, a fine lavoro, dovrà essere riposto in armadi o cassetti chiusi a chiave. Durante le normali quotidiane operazioni di lavoro, infine, non dovrà risultare visibile a persone non incaricate degli stessi trattamenti.

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

INFORMATIVA AI SENSI DEL REGOLAMENTO (UE) 679/2016 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Ai sensi degli articoli 13 e 14 del Regolamento (UE) 679/2016 in materia di protezione dei dati personali (in seguito, GDPR), Banca Monte dei Paschi di Siena S.p.A. (in seguito, la Banca), in qualità di Titolare del trattamento, La informa circa l'utilizzo dei Suoi dati personali nonché sui diritti a Lei riconosciuti, affinché possa manifestare in maniera libera e consapevole il Suo consenso, ove richiesto.

1. **Fonte dei dati personali**

I dati personali a Lei riferiti (a titolo esemplificativo, dati anagrafici, residenza, recapiti telefonici, titolo di studi) sono raccolti dalla Banca direttamente presso di Lei ovvero sono acquisiti presso terzi (ad esempio, tramite l'istituto scolastico presso cui Lei è iscritto) e vengono trattati nel rispetto del citato GDPR e degli obblighi di riservatezza e sicurezza ai quali si attiene la Banca. Nel caso in cui lei sia minorenne, potrebbero essere richiesti anche i dati personali dei Suoi familiari.

2. **Finalità del trattamento dei dati**

I Suoi dati personali sono trattati dalla Banca esclusivamente per finalità strettamente connesse e strumentali alla gestione del rapporto di lavoro, ivi comprese le finalità previdenziali, quali ad esempio:

- l'adempimento di obblighi previsti dalla legge, da un regolamento, dalla normativa comunitaria e secondaria;
- l'esecuzione di obblighi derivanti dal Suo contratto di lavoro, ai fini del Suo corretto inquadramento aziendale e quindi per assolvere a tutte le necessità e agli obblighi di legge in materia di tirocini formativi e di orientamento (DM 142/98), ovvero in relazione a contratti di somministrazione o altra natura.

Per tali finalità non è richiesto il Suo preventivo consenso, in quanto Lei ha l'obbligo legale e contrattuale di fornire i dati personali: ne consegue che qualora i dati non vengano forniti la Banca non potrà eseguire il contratto di lavoro o di qualsivoglia natura con lei instaurato. Al riguardo, pertanto, in relazione al trattamento dei dati è lecito considerare che ricorra almeno una delle seguenti condizioni:

- il trattamento è necessario all'esecuzione del contratto di lavoro con Lei instaurato (in tale contesto, ove previsto, potranno essere trattati dati personali relativi ai Suoi familiari);
- il trattamento è necessario per adempiere ad un obbligo di Legge al quale è soggetto il titolare del trattamento;
- il trattamento dei dati risulta altresì necessario per il perseguimento del legittimo interesse del titolare del trattamento alla gestione del rapporto di lavoro, nel rispetto dei diritti e delle libertà fondamentali del lavoratore ed in conformità ai principi di proporzionalità e necessità (ad esempio, nel rispetto della normativa di riferimento a tutela del patrimonio aziendale, mediante l'adozione ed utilizzo di sistemi di sicurezza e videosorveglianza; trasmissione dei dati personali all'interno di un gruppo imprenditoriale ai fini amministrativi interni).

3. **Categorie particolari di dati**[1]

[1] *Definizione di "categorie particolari di dati personali:" i *dati personali che rivelino l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, nonché i trattamenti di dati genetici, biometrici intesi a identificare in modo univoco una persona*

Può accadere che per l'adempimento di specifici obblighi relativi alla gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e di previdenza e assistenza, la Banca possa venire a conoscenza di dati che la Legge definisce come "categorie particolari di dati", in quanto gli stessi sono idonei a rivelare le convinzioni religiose (fruizione, prevista dalla legge, di permessi in occasione di festività religiose), l'adesione a partiti politici (richiesta di permessi o aspettative per la copertura di cariche pubbliche elettive), l'iscrizione a sindacati (assunzione di cariche sindacali; versamento di quote ad associazioni sindacali), lo stato di salute (presentazione di certificati medici relativi alle assenze per malattia, maternità, infortunio, certificazione di idoneità allo svolgimento di determinate mansioni), nonché di informazioni relative a provvedimenti di cui è prevista l'iscrizione nel casellario giudiziale.
Rispetto al trattamento di tali dati Le segnaliamo che il divieto non si applica qualora lo stesso trattamento sia necessario per assolvere agli obblighi ed esercitare i diritti del Titolare o dell'interessato in materia di diritto del lavoro, della sicurezza e protezione sociale, nella misura in cui sia autorizzato dalla legge, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi del dipendente.

4. Modalità di trattamento dei dati

Il trattamento dei Suoi dati personali avviene mediante strumenti informatici, telematici e manuali, con logiche strettamente correlate alle finalità sopra indicate e, comunque, nel rispetto di misure tecniche ed organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio.

5. Categorie di soggetti ai quali i dati possono essere comunicati

La Banca può comunicare i Suoi dati a determinati soggetti terzi, ubicati all'interno e/o all'esterno dell'UE, qualora vi sia un preciso obbligo normativo che ne impone la comunicazione, oppure perché la Banca si avvale di detti soggetti - a cui deve necessariamente comunicare i Suoi dati - per lo svolgimento di talune attività connesse alla gestione del Suo rapporto di lavoro. Si tratta di persone fisiche o giuridiche che ricoprono il ruolo di Responsabile esterno o di Titolare autonomo del trattamento. Di seguito si riportano le categorie dei soggetti a cui possono essere comunicati i Suoi dati:

- istituti di previdenza e assistenza (INPS, INAIL);
- autorità che ne facciano richiesta per l'espletamento delle attività funzionali ad esse attribuite per legge (amministrazione finanziaria, polizia giudiziaria, organi preposti alla vigilanza in materia di igiene e sicurezza sul lavoro);
- compagnie di assicurazione;
- società anche situate all'estero che svolgono servizi bancari e finanziari, appartenenti o meno al Gruppo Bancario MPS, ovvero controllate o collegate ai sensi dell'art. 2359 del Codice Civile, ovvero sottoposte a controllo, quando tale comunicazione sia consentita da un provvedimento del Garante della Privacy, o sia effettuata per finalità amministrativo-contabili previste dal GDPR e in tutti casi in cui si sia in presenza di uno dei presupposti di liceità del trattamento previsti dallo stesso GDPR;
- società ed imprese di servizi (ad esempio, in relazione alla gestione delle missioni/trasferte, per la fruizione di corsi di aggiornamento, la spedizione della corrispondenza);
- consulenti e liberi professionisti (ad esempio, docenti che tengono corsi nelle strutture della Banca).

Il suddetto elenco è conservato e costantemente aggiornato a cura della **Funzione ICT Compliance** a cui può rivolgersi ai recapiti di seguito indicati per qualsiasi informazione al riguardo.

Inoltre, possono venire a conoscenza dei Suoi dati personali il personale della Banca nonché suoi collaboratori designati Responsabili e/o incaricati del trattamento ai sensi del GDPR (ad esempio, il Servizio

---

fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (art. 9 del GDPR).

Knowledge, Management, Formazione e/o delle Funzioni aziendali presso le quali svolgerà il Suo tirocinio formativo o il rapporto lavorativo scaturente da contratti di somministrazione o di altra natura), i quali nell'ambito delle mansioni loro affidate, hanno accesso ai Suoi dati.

Inoltre, ferme restando le comunicazioni e diffusioni effettuate in esecuzione di obblighi di legge, di regolamento o di normativa comunitaria, La informiamo, altresì, che le eventuali tesi sviluppate presso la nostra Banca potranno essere pubblicate attraverso canali di comunicazione interna del Gruppo MPS. Fatte salve tali possibilità, i Suoi dati non verranno diffusi a terzi ma potranno essere comunicati a quei soggetti che hanno necessità di accedervi per finalità connesse e strumentali alla gestione del rapporto che intercorre tra Lei e la Banca e nei limiti strettamente necessari per svolgere tali finalità (Università presso cui è iscritto, Ente di formazione che ha promosso lo stage, etc.).

6. Trasferimento dei dati all'estero

Per finalità connesse alla gestione del rapporto di lavoro, i Suoi dati personali possono essere trasferiti all'estero, all'interno e/o all'esterno dell'Unione Europea, sempre nel rispetto dei diritti e delle garanzie previsti dalla normativa vigente in materia di protezione dei dati personali (capo V - Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali del GDPR).
Rientra in tali casi 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. Al riguardo si precisa che in relazione agli eventuali dati archiviati in stabilimenti o data center di proprietà del fornitore ubicati negli USA e potenzialmente accessibili alle autorità statunitensi - seppur nei limiti del c.d. accordo "Privacy Shield" definito con la UE – la Banca adotta con il fornitore del servizio misure volte a garantire la confidenzialità e sicurezza dei dati stessi.
Inoltre, qualora per questioni di natura tecnica e/o operativa si renda necessario avvalersi di soggetti ubicati al di fuori dell'Unione Europea, la informiamo sin d'ora che tali soggetti saranno nominati Responsabili del Trattamento ai sensi dell'art. 28 del GDPR.

7. Tempo di conservazione dei dati

I Suoi dati vengono conservati per il tempo strettamente necessario all'adempimento delle finalità per cui sono stati raccolti, nel rispetto dei termini prescrizionali o dei diversi termini eventualmente stabiliti dalla normativa legale e regolamentare di riferimento o necessari per esigenze di giustizia o di pubblico interesse.

8. Diritti dell'interessato

In relazione ai trattamenti sopra descritti, Le è riconosciuto l'esercizio dei diritti previsti dall'art. 15 e seguenti del GDPR, in particolare il diritto di:

- **accesso**, ovvero di ottenere la conferma dell'esistenza o meno di dati personali che La riguardano, di conoscerne l'origine, nonché la logica e le finalità su cui si basa il trattamento, i destinatari o le categorie di destinatari a cui i dati possono essere comunicati, la determinazione del periodo di conservazione qualora sia possibile definirlo;
- **rettificare** i dati inesatti;
- **cancellazione** (c.d. diritto all'oblio), nel caso in cui i dati non siano più necessari rispetto alle finalità della raccolta e successivo trattamento, ovvero nel caso in cui l'interessato abbia revocato il consenso al trattamento (laddove detto consenso sia previsto come facoltativo ovvero non sussista altro fondamento giuridico per il trattamento);
- **limitazione**, il diritto di ottenere da parte della Banca la limitazione dell'accesso ai dati personali da parte di tutti i soggetti che hanno un contratto di servizio ovvero un contratto di lavoro con la Banca. In

alcuni casi la Banca si riserva di consentire l'accesso ad un ristretto numero di persone allo scopo di garantire comunque la sicurezza, l'integrità e la correttezza dei suddetti dati;

- **portabilità**, il diritto di ricevere in un formato strutturato e di uso comune e leggibile da dispositivo automatico i dati personali che riguardano l'interessato, con possibilità di trasmetterli ad un altro Titolare. Tale diritto non si applica ai trattamenti non automatizzati (ad esempio, archivi o registri cartacei); inoltre, sono oggetto di portabilità solo i dati trattati con il consenso dell'interessato e solo se i dati sono stati forniti dall'interessato medesimo;
- **opposizione**, cioè il diritto di opporsi al trattamento per motivi connessi alla Sua situazione particolare tra cui vi rientra anche il diritto di opporsi al trattamento di dati personali ai fini di invio di materiale pubblicitario o newsletter, di vendita diretta o per il compimento di ricerche di mercato, di rilevazione del grado di soddisfazione e per i trattamenti connessi all'attività di profilazione. Il diritto di opposizione si riterrà esteso alla ricezione delle comunicazioni promozionali effettuate sia con i sistemi tradizionali che automatizzati, salva la possibilità di esprimere il Suo consenso per le sole modalità di contatto tradizionali;
- **reclamo** da inviare al Garante per la Protezione dei dati personali, piazza di Monte Citorio n. 121 – 00186 Roma (garante@gpdp.it; telefono + 39 06 69677.1; fax + 39 06 69677.3785).

Inoltre, ai sensi dell'art.7, co.3 del GDPR l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento; la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

Per l'esercizio dei diritti di cui sopra potrà rivolgersi alla Funzione ICT Compliance, Via Lippo Memmi n. 14 - 53100 Siena (fax + 39 0577 296520; e-mail: privacy@mps.it). Presso tale Funzione è disponibile l'elenco completo ed aggiornato dei Responsabili, interni ed esterni alla Banca.

9. Titolare del trattamento e Responsabile della Protezione dei Dati

Titolare del trattamento è la Banca Monte dei Paschi di Siena S.p.A. con sede a Siena in Piazza Salimbeni n. 3.

Il Responsabile della Protezione dei Dati (o, Data Protection Officer-DPO) è il Responsabile pro tempore della Funzione ICT Compliance, contattabile ai seguenti recapiti di posta certificata responsabileprotezionedeidati@postacert.gruppo.mps.it e di posta ordinaria responsabileprotezionedeidati@mps.it, a cui l'interessato può rivolgersi per tutte le questioni relative al trattamento dei propri dati personali e per l'esercizio dei diritti previsti dal GDPR.

Banca Monte dei Paschi di Siena S.p.A.

Il sottoscritto JAHELEZI XHUANA dichiara di aver preso visione dell'Informativa di cui sopra.

Firma

Data 28-01-2019