SINTESI POLITICA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Maggio 2018

Indice

1 Obiettivo del documento

La presente politica (di seguito "Politica") è redatta in ottemperanza all'art. 24, comma 2, del Regolamento (UE) 2016/679 ("GDPR" o "Regolamento") che abroga la precedente Direttiva 95/46/CE e disciplina gli aspetti relativi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi.

La Politica definisce:

(i) i principi generali applicabili a Spafid Connect, in qualità di titolare del trattamento di dati personali e i presìdi generali adottati per ottemperare a tali principi;

(ii) le responsabilità e i compiti degli organi sociali e delle strutture aziendali di Spafid Connect.

La Funzione Compliance di Spafid Connect - d'intesa con l'unità Group Data Protection Officer della Capogruppo Mediobanca - provvede, con cadenza almeno annuale, a rivedere la Politica e a valutare eventuali modifiche da apportare. Ogni modifica sostanziale del documento deve essere approvata dal Consiglio di Amministrazione di Spafid Connect.

Eventuali modifiche derivanti da i) cambiamenti organizzativi, ii) emanazione o modifica della normativa di secondo livello (es. Provvedimenti del Garante Privacy) sono apportate, su proposta della Funzione Compliance di Spafid Connect - d'intesa con la citata unità Group Data Protection Officer - dall'Amministratore Delegato, con informativa al Consiglio di Amministrazione e al Collegio Sindacale, nell'ambito delle relazioni periodiche della Funzione Compliance.

La Politica entra in vigore il 25 maggio 2018, sarà pubblicata sulla intranet aziendale e uno stralcio della stessa afferente ai principi generali sul trattamento dei dati personali sarà pubblicato sul sito internet di Spafid Connect.

2 Principi e presidi generali sul trattamento di dati personali

La Politica identifica i principali presìdi individuati da Spafid Connect per assicurare il rispetto dei principi generali contenuti nel GDPR, con particolare riguardo a (i) liceità del trattamento, (ii) diritti degli interessati; (iii) registro dei trattamenti e valutazione d'impatto sulla protezione dei dati; (iv) sicurezza dei trattamenti e (v) gestione degli eventi di data breach. Al riguardo Spafid Connect:

(i) adotta processi, strumenti e controlli idonei, che consentano il pieno rispetto dei principi generali sul trattamento dei dati personali;

(ii) garantisce adeguati flussi informativi da e verso gli organi sociali, le strutture di controllo e operative;

(iii) assicura lo svolgimento delle attività di formazione del personale in materia di protezione dei dati personali, al fine di garantire il rispetto della normativa applicabile da parte di chiunque ponga in essere attività di trattamento dei dati personali all'interno della struttura aziendale sotto l'autorità del titolare.

I trattamenti di dati personali delle diverse categorie di soggetti interessati (es. clienti, dipendenti, visitatori, fornitori) svolti da Spafid Connect si fondano sui seguenti principi:

- **liceità, correttezza e trasparenza**: i dati personali sono raccolti e trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

- **limitazione della finalità**: i dati personali sono raccolti e trattati per finalità determinate, esplicite e legittime;

- **minimizzazione dei dati**: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

- **esattezza**: i dati personali sono mantenuti esatti ed aggiornati e sono adottate misure ragionevoli per cancellare o rettificare, tempestivamente, i dati inesatti o superati;

- **limitazione della conservazione (c.d. data retention)**: i dati personali sono conservati per un arco temporale non superiore al conseguimento delle finalità per cui sono stati raccolti;

- **integrità e riservatezza**: i dati personali sono trattati in modo da garantirne un'adeguata sicurezza, attraverso l'adozione di misure tecniche ed organizzative adeguate;

- **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. Mediobanca deve trattare, di default, solamente quei dati che siano necessari al perseguimento delle finalità del trattamento;

- **responsabilizzazione (c.d. accountability)**: i trattamenti dei dati personali sono svolti secondo i principi che precedono e il loro rispetto è adeguatamente documentato.

2.1. Liceità del trattamento

I trattamenti di dati personali all'interno di Spafid Connect possono essere condotti esclusivamente sulla base di una o più delle seguenti condizioni:

- contratto di cui l'interessato è parte;

- obbligo legale cui è soggetta Spafid Connect ;

- salvaguardia di interessi vitali del soggetto interessato;

- esplicito consenso dell'interessato;

- perseguimento di un legittimo interesse di Spafid Connect.

2.1.1. Richiesta del consenso

Laddove il trattamento di dati personali si fondi sul consenso dell'interessato, la raccolta del consenso è effettuata tramite dichiarazione scritta ovvero, in casi particolari caratterizzati da minore rischiosità, in forma orale e documentata per iscritto. Qualora nel modulo utilizzato per la raccolta del consenso si trattino altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice in modo tale che la volontà dell'interessato sia liberamente espressa. Il consenso è revocabile in qualsiasi momento e la sua revoca non pregiudica la liceità del trattamento effettuato fino a quel momento.

2.1.2. Legittimo interesse

In alcuni casi le procedure di Spafid Connect devono prevedere che il trattamento di dati personali possa essere effettuato al fine di perseguire un legittimo interesse di Spafid Connect. In ottemperanza al principio di accountability, in tali casi, le procedure devono prevedere che la valutazione circa il corretto bilanciamento tra gli interessi di Mediobanca e i diritti dell'interessato sia adeguatamente documentata.

2.1.3. Trasferimento di dati all'estero

Il trasferimento di dati personali verso un paese terzo (non appartenente all'Unione) o un'organizzazione internazionale può avere luogo senza autorizzazioni specifiche solo se la Commissione Europea ha deciso che il paese terzo o l'organizzazione internazionale garantisce un livello di protezione adeguato, sulla base di una serie di elementi (tra cui il rispetto dei diritti umani e delle libertà fondamentali, l'esistenza e l'effettivo funzionamento delle Autorità di controllo).

In mancanza di una decisione di adeguatezza[1], la Società può trasferire i dati personali solo se ha fornito garanzie adeguate[2] e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

2.2. Diritti degli interessati

2.2.1. Informativa sul trattamento

In conformità ai principi di trasparenza, correttezza, limitazione delle finalità e data retention, le procedure devono prevedere che ai soggetti interessati, all'atto della raccolta dei dati personali, vengano fornite chiare informazioni (**Informativa**) circa: i) l'identità di Spafid Connect e del Responsabile della Protezione dei Dati[3] ("DPO – Data Protection Officer"), ii) le caratteristiche del trattamento (es. le finalità e la base giuridica dello stesso, il periodo di conservazione dei dati) e iii) i diritti del soggetto interessato.

Qualora i dati non siano stati ottenuti presso l'interessato, l'informativa indica anche la fonte da cui hanno origine i dati personali e se si tratta di dati provenienti da fonti accessibili al pubblico.

2.2.2. Diritti d'accesso, rettifica, cancellazione, portabilità e opposizione

Le procedure devono assicurare il rispetto del principio di esattezza e di data retention, prevedendo che ogni interessato abbia il diritto di ottenere:

(i) la conferma che siano o meno in corso attività di trattamento di suoi dati personali e informazioni sulle caratteristiche del trattamento (es. finalità, categorie di dati personali, destinatari della comunicazione dei dati, diritti dell'interessato);

(ii) la rettifica di dati personali inesatti che lo riguardano, nonché la loro integrazione qualora siano incompleti;

(iii) la cancellazione, se sussistono alcune fattispecie, ad esempio se i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti, se l'interessato ha

[1] Sulla base della Direttiva 95/46/CE sono state emesse 14 decisioni di adeguatezza: Andorra, Argentina, Australia, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, USA (dal 2016 – Privacy Shield).
[2] Ad esempio, le clausole tipo di protezione dei dati adottate dalla Commissione (c.d. "standard contract rules").
[3] Il DPO costituisce un elemento chiave all'interno del nuovo sistema di governance dei dati e ad esso sono attribuiti dal GDPR compiti generali di facilitare e favorire l'osservanza della normativa attraverso strumenti di accountability e fungere da interfaccia tra i vari soggetti coinvolti (autorità di controllo, interessati e divisioni operative all'interno della struttura aziendale).

revocato il consenso o ha esercitato il diritto di opposizione al trattamento, oppure se i dati personali sono stati trattati illecitamente;

(iv) la portabilità dei dati oggetto del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, qualora il trattamento si basi su un consenso legittimo e sia effettuato con mezzi automatizzati;

(v) la cessazione del trattamento dei dati nel caso di trattamento effettuato sulla base del consenso dell'interessato.

Le procedure devono prevedere che, a seguito di ciascuna richiesta, si debbano fornire agli interessati le informazioni necessarie in forma concisa, accessibile ed usando un linguaggio semplice e chiaro, entro un mese (estendibile fino a due mesi, in casi di particolare complessità), anche in caso di diniego.

2.3. Registro dei trattamenti, analisi dei rischi, valutazione d'impatto e consultazione preventiva

Spafid Connect è tenuta a predisporre e aggiornare periodicamente un "registro delle attività di trattamento" che identifichi le attività svolte in qualità di titolare o di responsabile del trattamento. Il registro costituisce la mappatura di tutti i trattamenti effettuati e viene aggiornato periodicamente. Il registro deve essere reso disponibile su richiesta all'Autorità di Controllo. Il registro rappresenta la base per assicurare il rispetto dei principi generali sanciti dal GDPR.

Al fine di assicurare l'integrità e la riservatezza dei dati personali, per ciascuna attività di trattamento identificata nel registro, viene effettuata un'analisi del rischio. Ove da tale analisi emerga che il trattamento possa comportare un livello di rischio elevato per i diritti e le libertà degli interessati, le procedure devono prevedere lo svolgimento di una valutazione di impatto sulla protezione dei dati (Data Protection Impact Assessment, di seguito "DPIA"), previo consulto con il DPO.

In particolare, le procedure devono prevedere che, nel valutare la necessità di effettuare una DPIA su un determinato trattamento, si tenga conto: (i) del livello di rischio per i diritti e le libertà degli interessati, (ii) dell'esistenza di un trattamento automatizzato (inclusa la profilazione); (iii) del fatto che il trattamento sia effettuato su larga scala o (iv) possa comportare la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

2.4. Sicurezza del trattamento

Per garantire un livello di sicurezza del trattamento dei dati adeguato al rischio, le procedure devono definire misure tecniche e organizzative, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi del trattamento e alla natura dei dati personali, in accordo ai principi di "privacy by design" e "privacy by default". Queste misure possono comprendere:

- la pseudonimizzazione e la cifratura dei dati personali;
- la riservatezza e l'integrità dei sistemi e dei servizi di trattamento assicurate su base permanente;
- meccanismi di verifica e valutazione della loro efficacia.

Tenendo conto dei rischi presentati dal trattamento che derivano, in particolare, dalla distruzione, dalla perdita o dalla modifica non autorizzata di dati personali, le procedure devono definire le misure di sicurezza che possono garantire un adeguato livello di

protezione dei dati personali di default e in via preventiva rispetto allo stesso trattamento dei dati personali.

2.5. Gestione degli eventi di data breach

Sempre al fine di assicurare il rispetto dei principi di integrità e riservatezza dei dati personali, laddove sia identificata una violazione di sicurezza, accidentale o illecita, che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati compromettendone la riservatezza, la disponibilità o l'integrità, le procedure devono assicurare, previo coinvolgimento del DPO, che la notifica all'Autorità di Controllo avvenga entro 72 ore dal momento in cui sia stata ravvisata la violazione. Tale notifica contiene:

- la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati;
- i dati di contatto del DPO;
- le probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

Qualora la notifica non sia effettuata entro 72 ore, devono essere indicati i motivi del ritardo.

Nei casi in cui la violazione possa comportare elevati rischi per i diritti e le libertà dei soggetti interessati, le procedure devono prevedere che - previo consulto con il DPO, sia fornita agli interessati informativa sulla violazione senza ingiustificato ritardo. Tale comunicazione non è necessaria se comporterebbe uno sforzo sproporzionato oppure se sono state adottate misure tecniche ed organizzative adeguate alla tutela dei dati (es. cifratura).

Le procedure devono stabilire che: (i) la scelta della modalità di comunicazione dovrà tenere in considerazione l'accessibilità dei soggetti interessati a formati diversi, e, ove necessario, le diversità linguistiche dei destinatari; e (ii) ciascuna violazione dei dati personali, sospetta o accertata, deve essere adeguatamente censita e documentata nel registro delle violazioni al fine di garantire il rispetto del principio di accountability.

3 Ambito di applicazione e modello di Gruppo

L'applicazione della disciplina al Gruppo Mediobanca avviene sulla base del seguente modello:

- Mediobanca, in quanto soggetto che effettua trattamenti di dati personali (es. clienti, dipendenti, visitatori, fornitori) nell'Unione Europea, nonché tutte le società controllate italiane del Gruppo che effettuano trattamenti di dati personali applicano integralmente il GDPR, unitamente alla regolamentazione italiana (cluster 1);
- le società controllate estere stabilite nell'UE che trattano dati personali e le società controllate estere che non sono stabilite nell'UE, ma che offrono beni o servizi – esclusivamente o anche solo in parte – a persone fisiche che si trovano nell'UE, trattando i loro dati, applicano il GDPR, unitamente alla regolamentazione locale di riferimento (cluster 2);
- le società controllate estere non rientranti nelle fattispecie precedenti, ove procedano al trattamento di dati personali, rientrano nel cluster 3.

La Politica trova quindi applicazione integrale per il cluster 1 e, previo adattamento al contesto nazionale di riferimento, per il cluster 2. Con riferimento al cluster 3, identifica i principi cardine cui si ispira il Gruppo e deve essere applicata, anche in tale circostanza previo adeguamento alla disciplina locale, secondo un principio di proporzionalità, con particolare riferimento ai presidi descritti al paragrafo 2.

Il presidio del rischio correlato al trattamento dei dati personali è assicurato: per il cluster 1, attraverso i) l'adozione dei presìdi generali contenuti nella presente Politica e ii) la nomina del medesimo DPO, facoltà concessa dall'art. 37 del GDPR; peri cluster 2 e 3, attraverso il coordinamento tra il DPO di Mediobanca e il referente locale Compliance ovvero il DPO della società, ove nominato.

Allegato 1 – Principali definizioni

Dati personali	Tutte le informazioni relative a persone fisiche che consentano l'identificazione, diretta o indiretta, degli individui a cui i dati si riferiscono. Ad esempio, sono dati personali oggetto di tutela, oltre ai dati anagrafici ed economici, anche le immagini ed i codici identificativi riconducibili ad un individuo
Categorie particolari di dati personali	Dati capaci di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale
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 relativi a condanne penali e a reati	Dati relativi a condanne penali e reati o a connesse misure di sicurezza. Il loro trattamento è ammesso solo sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'UE o degli Stati membri, in presenza di garanzie appropriate per i diritti e le libertà degli interessati
Dati biometrici	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
Dati genetici	Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica
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
Archivio	Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentrato o ripartito in modo funzionale o geografico
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento
Contitolare del trattamento	La persona fisica o giuridica che determina congiuntamente ad uno o più titolari le finalità e i mezzi del trattamento. I contitolari definiscono i rispettivi ambiti di responsabilità e compiti in un accordo scritto
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. E' nominato dal titolare, qualora un trattamento debba essere effettuato per suo conto
Sub-responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del responsabile del trattamento, previo ottenimento della richiesta di autorizzazione scritta, specifica o generale, del titolare del trattamento
Incaricato/Addetto autorizzatio	Il soggetto che tratta dati personali sotto l'autorità del titolare del trattamento o del responsabile del trattamento su loro specifiche istruzioni

Amministratore di sistema	Le persone incaricate di gestire e mantenere gli impianti di elaborazione di dati personali o sue componenti. L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento di dati personali. La designazione ad amministratore è individuale e reca l'elencazione analitica degli ambiti di operatività in base al profilo di autorizzazione assegnato
Responsabile della protezione dei dati personali (DPO)	La persona fisica che deve essere designata dal titolare del trattamento e dal responsabile del trattamento, in specifici casi (ad esempio, se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala)
Rappresentante	La persona fisica o giuridica stabilita nell'Unione Europea che, designata per iscritto dal titolare del trattamento/responsabile del trattamento non stabilito nell'EU, li rappresenta per quanto riguarda gli obblighi di cui al GDPR
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere caratteristiche riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica
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
Cifratura	Modalità di conversione del testo originale in una sequenza apparentemente casuale di lettere, numeri e segni speciali che solo la persona in possesso della corretta chiave di decifratura potrà riconvertire nel file di testo originale
Violazione dei dati personali (*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
Autorità di controllo	L'autorità pubblica indipendente istituita da uno Stato membro con lo scopo di sorvegliare l'applicazione della normativa sulla protezione dei dati personali, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali
Dipendenti	Ogni dipendente di Spafid Connect assunto con contratto a tempo indeterminato o determinato, full time o part time, al personale in somministrazione lavoro o staff leasing, stagisti e collaboratori, comprese le filiali estere