Policy in materia di protezione dei dati personali

Modena, *24/11/2022*

Versione 3.0

INDICE

1 Aspetti Generali

Sintesi principali tematiche trattate / modifiche apportate:

La presente Policy definisce i requisiti per il trattamento dei Dati Personali nell'ambito del Gruppo Bper; disciplina le regole e i presidi che Bper Banca, in qualità di Capogruppo, ha indicato per le Società del Gruppo Bper con l'obiettivo di assicurare protezione ai Dati Personali e tutelare i diritti e le libertà degli Interessati. Bper e le Società del Gruppo hanno impostato le attività inerenti ai Trattamenti conformemente alla Normativa in materia di protezione dei Dati Personali e in linea con i valori etici e di comportamento, nonché di sostenibilità anche definiti nel Codice Etico e di Condotta di Gruppo.

Nell'ottica di assicurare un costante allineamento con i requisiti derivanti dalla normativa in materia di protezione dei Dati Personali tempo per tempo cogente, il documento sarà oggetto di revisione e aggiornato ogniqualvolta intervengano modifiche rilevanti del contesto interno o esterno di riferimento.

La precedente versione del documento è stata rivisitata e definisce più puntualmente i requisiti, le misure nonché i principi applicabili al trattamento dei Dati Personali per la protezione e tutela dei diritti e delle libertà fondamentali dei soggetti Interessati.
In particolare, tra l'altro, ha meglio regolamentato: la necessità di condurre un Legitimate Interest Assessment per i trattamenti di dati personali il cui presupposto di liceità si identifichi nel legittimo interesse del titolare; l'individuazione di circostanze in cui la normativa consente il trattamento di dati particolari e di quelli giudiziari prevedendo l'adozione di misure di sicurezza rafforzate a protezione di tali dati; l'utilità di fornire ai soggetti autorizzati istruzioni circa i trattamenti di dati personali tramite apposita nomina.
Le modalità di presidio del rischio Privacy contenute all'interno della Policy risultano mutuate anche per le altre società del Gruppo Bper quali destinatarie del documento.

Redattore:

Ufficio Privacy & Data Protection

Approvatore:

CdA

Destinatari del documento:

Banche		Società					
Allineate informaticamente		Strumentali		Finanziarie		Altre società controllate*	
X	Bper	X	MO Terminal	-	Di Credito		Adras
X	Bibanca	X	Bper Real Estate	X	Bper Factor		Ivi
X	Banco di Sardegna	X	Numera	X	Sardaleasing		Sifà
Non allineate informaticamente		X	Bper Credit Management	X	Finitalia		Arca Holding
X	Banca Carige	X	Carige Reoco	X	Lanterna Lease		
X	Banca del Monte di Lucca	X	Bper Trust Company	-	Non di Credito		
X	Banca Cesare Ponti	X	Argo Mortgage 2	X	Estense C. Bond		
				X	Estense		

					C.B.CPT		
		X	Centro Fiduciario CF 2	X	Carige CB 2		
Estere				X	Optima Sim		
	Bper Lux				Arca Fondi SGR		

*rientranti nel perimetro di consolidamento ma non facenti parte del Gruppo Bancario

Albero dei Processi:

Albero dei Processi	Descrizione
Area	Processi direzionali
Macroprocesso	Adempimenti normativi privacy e data protection

2 Definizioni

Salvo quanto diversamente previsto all'interno del documento, tutti i termini riportati con lettera iniziale maiuscola si riferiscono alle definizioni presenti nel GDPR e/o nei provvedimenti vigenti, riportate nel seguito per comodità:

- **Autorità di Controllo**: autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR.
- **Consenso**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento.
- **Dati Personali:** 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.
- **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.
- **Dati Giudiziari:** Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
- **Dati Particolari:** categorie particolari di Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, e/o biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Destinatario**: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Non sono considerate Destinatari le Autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri.
- **Delegato Privacy**: è incardinato nella figura dell'Amministratore Delegato, che ha in capo l'attuazione, in piena autonomia operativa e con facoltà decisionale anche sotto il profilo della capacità di spesa, delle misure tecniche/organizzative necessarie a norma degli articoli 24 e 32 del Regolamento, con conseguente assunzione di ogni relativa responsabilità, per garantire ed essere in grado di dimostrare che il Trattamento dei Dati Personali è effettuato conformemente alla normativa vigente.
- **DPO** o **Data Protection Officer**: figura incaricata di svolgere, in piena autonomia e indipendenza, i compiti e le funzioni di cui all'articolo 39 par 1 del GDPR e deputata, altresì a facilitare l'osservanza della normativa di riferimento in materia di protezione dei Dati Personali. La nomina di un DPO è obbligatoria per tutti i soggetti pubblici e per altri soggetti le cui attività principali consistano in Trattamenti che per loro natura, ambito di applicazione e finalità richiedono il monitoraggio regolare e sistematico degli Interessati ovvero nel Trattamento, su larga scala, di categorie particolari di Dati Personali (ref. Art. 37.1 GDPR).

- **GDPR (**o **Regolamento):** Regolamento Generale sulla Protezione dei Dati Personali (UE) 2016/679.
- **Incaricato o Soggetto Autorizzato:** soggetto che effettua trattamenti di Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile del Trattamento. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori della Società e, più in generale, tutti coloro che Trattano Dati Personali di clienti, dipendenti e fornitori.
- **Normativa in materia di protezione dei Dati Personali:** il novero di Regolamenti, Leggi, Decreti, Raccomandazioni, Linee Guida e Provvedimenti in materia di protezione dei Dati Personali applicabili al Gruppo Bper, come identificati nel paragrafo 7.2.
- **Processo Decisionale Automatizzato:** decisione basata unicamente sul Trattamento di Dati Personali automatizzato, compresa la profilazione, che produca effetti giuridici che riguardano l'Interessato al quale i dati si riferiscono o che incida in modo analogamente significativo sulla sua persona.
- **Profilazione:** qualsiasi forma di Trattamento automatizzato consistente nell'utilizzo di Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
- **Pseudonimizzazione:** il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano 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.
- **Rappresentante:** la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del Trattamento o dal Responsabile del Trattamento per iscritto ai sensi dell'articolo 27 GDPR, risulta essere il rappresentante degli obblighi riferibili al GDPR.
- **Responsabile del Trattamento** o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; tale figura presenta requisiti di idoneità per attuare le misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'Interessato.
- **Terzo:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del Trattamento, il Responsabile del Trattamento e le Persone Autorizzate al Trattamento dei Dati Personali sotto l'autorità diretta del Titolare o del Responsabile.
- **Titolare del Trattamento** o **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; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli stati membri.
- **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.
- **Violazione Dei Dati Personali** o **Data Breach:** è 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.

3 Contenuti della fonte normativa

La Normativa in materia di protezione dei Dati Personali definisce i requisiti, le misure nonché i principi applicabili al trattamento dei Dati Personali per la protezione e tutela dei diritti e delle libertà fondamentali dei soggetti Interessati. Ciascun Titolare è tenuto ad attuare tali requisiti, misure e principi per l'intero ciclo di vita

dei dati e dei trattamenti svolti su di essi ed essere in grado di dimostrare che il trattamento è effettuato nel rispetto della Normativa in materia di Protezione dei Dati Personali.

3.1 Principi applicabili al Trattamento dei dati

Liceità e correttezza

I Dati Personali devono essere trattati in modo lecito e corretto.

Nello specifico, è lecito il Trattamento di Dati Personali solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- l'Interessato ha espresso il consenso al Trattamento dei propri Dati Personali per una o più specifiche finalità;
- il Trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il Trattamento è necessario per adempiere a un obbligo legale al quale è soggetto il Titolare del Trattamento;
- il Trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
- il Trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento;
- il Trattamento è necessario per il perseguimento del legittimo interesse del Titolare del Trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato.

Trasparenza

I trattamenti di Dati Personali avvengono in un'ottica di piena trasparenza nei confronti dell'Interessato. Il Titolare del Trattamento è tenuto a fornire agli Interessati le informazioni di cui agli articoli 13 e 14 del GDPR e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, semplice, chiara, intelligibile e facilmente accessibile.

Il Titolare del Trattamento, inoltre, è tenuto ad agevolare l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22 del GDPR e a fornire le coerenti e dovute informazioni in merito al Trattamento dei Dati Personali, corredate con risposte chiare e complete.

Le comunicazioni effettuate dal Titolare all'Interessato in caso di Data Breach suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati descrivono con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contengono almeno le informazioni e le misure di cui all'articolo 33 del GDPR par 3, lettere b), c), d).

Limitazione della finalità

I Dati Personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

In caso di eventuali Trattamenti avviati successivamente alla raccolta dei dati è necessario valutare la coerenza tra le finalità perseguite e quelle comunicate al soggetto Interessato nell'ambito dell'informativa fornita. Tali valutazioni devono considerare almeno:

- ogni nesso tra le finalità per cui i Dati Personali sono stati raccolti e le finalità dell'ulteriore Trattamento previsto;
- il contesto in cui i Dati Personali sono stati raccolti, in particolare relativamente alla relazione tra l'Interessato e la Società;
- la natura dei Dati Personali, specialmente se sono Trattati Dati Particolari o Dati Giudiziari;
- le possibili conseguenze dell'ulteriore Trattamento previsto per gli Interessati;
- l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la Pseudonimizzazione.

Qualora dagli esiti delle analisi risulti che la nuova finalità di Trattamento non è coerente con le finalità

originarie, in applicazione del principio di trasparenza precedentemente definito, è necessario informare l'Interessato di tali finalità nonché dei diritti esercitabili, ivi compreso il diritto di opposizione laddove applicabile.

Minimizzazione dei dati

I Dati Personali devono essere pertinenti, adeguati e limitati a quanto necessario rispetto alle finalità per cui sono trattati.

Tale principio è attuato sia al momento di determinare i mezzi del Trattamento, sia all'atto del Trattamento, sia per l'intera durata del ciclo di vita del Trattamento stesso, assicurando che i soggetti autorizzati al Trattamento o designati Responsabili del trattamento abbiano accesso unicamente ai dati strettamente necessari per il perseguimento delle specifiche finalità.

Esattezza

I Dati Personali devono essere esatti e, se necessario, aggiornati, adottando misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per i quali sono stati trattati.

Anche nei casi in cui i Dati Personali non sono forniti direttamente dall'Interessato ma sono raccolti da soggetti terzi, permane la responsabilità di accertarsi della accuratezza e della qualità dei dati, nonché di attuare eventuali interventi per l'aggiornamento o la cancellazione dei dati inesatti.

Limitazione della conservazione

I Dati Personali sono conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per cui sono trattati. È pertanto necessario definire, per ciascuna finalità del Trattamento e per le diverse categorie di dati personali l'intervallo temporale per cui i dati devono essere conservati, trascorso il quale i dati devono essere cancellati o resi anonimi. È ammessa la conservazione dei dati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'Interessato.

Integrità e riservatezza

I Dati Personali, per l'intero ciclo di vita, sono trattati in maniera da garantire un'adeguata sicurezza dei Dati Personali compresa la protezione, adottando misure di sicurezza tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti nonché dalla perdita, distruzione o dal danno accidentali.

3.2 Presidi in materia di protezione dei Dati Personali

BPER Banca, in qualità di Capogruppo, è responsabile nel definire le linee di indirizzo in materia di protezione dei Dati Personali per l'intero Gruppo Bancario.

L'attuazione degli indirizzi formulati dalla Capogruppo avviene secondo principi di gradualità e proporzionalità in funzione delle specificità delle diverse società appartenenti al Gruppo e rientranti nel perimetro.

In applicazione del principio di responsabilizzazione ("accountability"), elemento cardine della Normativa in materia di protezione dei Dati Personali, il Gruppo BPER si è dotato di un insieme di regole interne e presidi volti ad assicurare che le operazioni di Trattamento siano condotte in modo trasparente e nel rispetto dei principi fondamentali e dei requisiti derivanti dalla Normativa in materia di protezione dei Dati Personali, nonché a comprovare tempo per tempo l'osservanza delle disposizioni normative.

3.1.1 Trattamento di Dati Particolari e Dati Giudiziari

Il Trattamento Dati Particolari è consentito unicamente in presenza di un consenso esplicito da parte dell'Interessato per una o più finalità specifiche, oltre che nella misura in cui il Trattamento:

- è esplicitamente consentito dal diritto nazionale ed europeo o da provvedimenti dell'Autorità di controllo in materia di protezione dei Dati Personali;
- è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del Trattamento o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dalla legge o dalla contrattazione collettiva nazionale in materia di lavoro;

- è necessario per tutelare un interesse vitale dell'Interessato o di un'altra persona fisica qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- riguarda Dati Personali resi manifestamente pubblici dall'Interessato;
- è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- è necessario per motivi di interesse pubblico rilevante sulla base del diritto nazionale o europeo;
- è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali.

Il Trattamento di Dati Giudiziari è consentito unicamente laddove esplicitamente autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:

- l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo;
- la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
- l'adempimento di obblighi e l'esercizio di diritti da parte del Titolare o dell'Interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro;
- la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
- l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
- l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
- l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti;
- la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
- l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
- l'attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese.

In considerazione del livello di riservatezza, per l'intero ciclo di vita del Trattamento, i Dati Particolari e i Dati Giudiziari sono protetti mediante l'adozione di misure di sicurezza tecniche e organizzative rafforzate.

3.1.2 Nomina dei Soggetti Autorizzati

I soggetti che, nello svolgimento delle attività di propria competenza, effettuano Trattamenti di Dati Personali sono designati Soggetti Autorizzati al Trattamento. La designazione avviene tramite apposito documento di nomina con cui il Titolare impartisce al Soggetto Autorizzato le istruzioni, riferibili all'ambito di assegnazione del soggetto, cui attenersi nel Trattamento di Dati Personali.

Inoltre, al fine di aumentare la consapevolezza dei Soggetti Autorizzati circa i requisiti in materia di protezione dei Dati Personali, il Titolare eroga periodicamente attività formative e campagne di sensibilizzazione sui presidi privacy adottati e la Normativa in materia di Protezione dei Dati Personali.

3.1.3 Informativa all'Interessato e raccolta del Consenso

L'Informativa contiene, di fatto, le informazioni richieste dalla Normativa in materia di protezione dei dati Personali, con particolare riferimento agli articoli 13 e 14.

Se i Dati Personali sono raccolti presso l'Interessato, l'Informativa è fornita nel momento in cui i dati personali sono ottenuti. Laddove invece i Dati Personali non sono raccolti direttamente presso l'interessato, l'informativa

è fornita entro un termine ragionevole dall'ottenimento dei dati personali, al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati e, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione.

L'informativa deve essere data in un formato chiaro, facilmente intellegibile e comprensibile dall'Interessato, e contenere tutte le informazioni richieste dalla normativa di riferimento, tra cui in particolare:

- l'identità e i dati di contatto del Titolare del Trattamento e, ove applicabile, del suo Rappresentante;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del Trattamento cui sono destinati i Dati Personali e il presupposto di liceità del Trattamento;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- i legittimi interessi perseguiti dal Titolare del Trattamento o da terzi, laddove il presupposto di liceità del Trattamento consista nel legittimo interesse;
- l'esistenza del diritto di revoca del Consenso in qualsiasi momento senza pregiudizio sulla liceità del Trattamento basata sul Consenso prestato prima della revoca, laddove il presupposto di liceità del Trattamento consista nel consenso dell'Interessato;
- gli eventuali destinatari o le eventuali categorie di destinatari dei Dati Personali;
- l'intenzione di trasferire dati personali a un paese terzo e l'esistenza o assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate adottate dal Titolare e i mezzi opportuni per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze previste di tale Trattamento per l'Interessato e il diritto di ottenere un intervento umano, di esprimere la propria opinione e di contestare la decisione;
- il periodo di conservazione dei dati personali oppure i criteri utilizzati per determinare tale periodo;
- il diritto dell'Interessato di chiedere al Titolare l'accesso, la rettifica, la limitazione del Trattamento, la portabilità o la cancellazione dei Dati Personali, nonché di opporsi al Trattamento e di proporre reclamo a un'Autorità di controllo.

Nei casi in cui il presupposto di liceità di un Trattamento è identificato nel Consenso dell'Interessato, lo stesso è acquisito in maniera:

- **libera**: senza condizionamenti o vincoli, assicurando la possibilità di revoca in ogni momento con la stessa facilità con cui il consenso è stato raccolto;
- **specifica**: in riferimento a ciascuna specifica finalità per cui il Consenso è necessario;
- **informata**: preceduto da una adeguata informativa che consenta all'Interessato di essere pienamente consapevole dei Trattamenti condotti sui Dati Personali ad esso riferiti;
- **inequivocabile**: il consenso è raccolto in modo chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'Interessato, assicurando la dimostrabilità del consenso prestato per la specifica finalità;
- **esplicita**: il consenso è fornito attraverso un'azione positiva o dichiarazione da parte dell'Interessato;
- **consapevole**: il consenso è considerato valido, coerentemente con quanto previsto dall'art. 2 quinquies del Codice Privacy, laddove fornito da soggetti maggiori di 14 anni di età. Laddove il Consenso riguardi soggetti di età inferiore ai 14 anni o soggetti appartenenti a categorie fragili, è necessario acquisire il Consenso da parte dei genitori, tutori o da chi ne fa le veci.

3.1.4 Valutazione del bilanciamento dei legittimi interessi del Titolare

Per i Trattamenti di Dati Personali il cui presupposto di liceità si identifichi nel legittimo interesse del Titolare, è necessario valutare, attraverso la conduzione di un Legitimate Interest Assessment, che gli interessi del Titolare non prevalgano i diritti e le libertà dell'Interessato, tenuto conto delle ragionevoli aspettative dell'Interessato in base alla sua relazione con il Titolare del Trattamento e dell'eventualità che l'Interessato, al momento e nell'ambito della raccolta dei Dati Personali, possa ragionevolmente attendersi un trattamento a tal fine.

Nell'ambito del Legitimate Interest Assessment, pertanto, sono tenuti in considerazione almeno i benefici che il Titolare o Terzi possano ricavare dal Trattamento, la natura della relazione tra il Titolare e l'Interessato, le ragionevoli aspettative dell'Interessato circa l'utilizzo dei relativi dati per il perseguimento della specifica finalità nonché gli eventuali impatti che il Trattamento potrebbe comportare per l'Interessato.

È possibile procedere con il Trattamento previsto unicamente in caso di esito positivo del Legitimate Interest Assessment. Laddove dalle valutazioni emerga invece che i diritti e le libertà dell'Interessato prevalgano gli interessi del Titolare, per la conduzione del Trattamento è necessario identificare un differente presupposto di liceità, valutando in particolare la possibilità di acquisire un consenso esplicito.

3.1.5 Tenuta ed aggiornamento del registro delle attività di Trattamento

Il Registro dei Trattamenti contiene una elencazione analitica delle attività di Trattamento condotte sotto la propria responsabilità, sia in qualità di Titolare sia in qualità di Responsabile, e indica almeno le informazioni richieste dalla normativa di riferimento, tra cui in particolare:

- il nome e i dati di contatto del Titolare del Trattamento e, ove applicabile, del Contitolare del Trattamento, del rappresentante del Titolare del Trattamento e del DPO;
- le finalità del Trattamento;
- una descrizione delle categorie di Interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale e la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative a protezione dei dati.

Il registro è costantemente manutenuto e aggiornato, in modo da assicurare piena coerenza con le attività di Trattamento effettivamente condotte.

3.1.6 Analisi di impatto sulla protezione dei dati

Nei casi in cui il Trattamento, in considerazione della natura, l'oggetto, il contesto, le finalità nonché le tecnologie utilizzate, possa presentare un rischio elevato per le persone fisiche, è necessario, prima di procedere al trattamento, condurre una valutazione di impatto dei trattamenti previsti sulla protezione dei dati (DPIA – Data Protection Impact Assessment), che comprenda almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del Trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del Trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli Interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità alla normativa di riferimento.

La valutazione di impatto è condotta preliminarmente all'avvio del Trattamento e revisionata con cadenza periodica o in caso di variazioni rilevanti del contesto in cui il Trattamento è condotto. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi analoghi.

Nell'ipotesi in cui dalla valutazione d'impatto sulla protezione dei dati risulti un elevato rischio in assenza di misure adottate per attenuare il rischio, prima di procedere al Trattamento, è necessario consultare il Garante per la protezione dei Dati Personali.

3.1.7 Adozione di adeguate misure a protezione dei dati

Per l'intera durata del relativo ciclo di vita, i Dati Personali sono adeguatamente protetti attraverso l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza coerente con la correlata rischiosità. Nel valutare il livello di sicurezza si tiene debitamente in conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o

dall'accesso, in modo accidentale o illegale, ai Dati Personali trattati.

Le misure di sicurezza adeguate devono essere determinate tenendo in considerazione lo stato dell'arte e i costi di attuazione, nonché la natura, l'oggetto, il contesto e le finalità del Trattamento, come anche il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

La Capogruppo ha individuato per il Gruppo misure organizzative e di sicurezza a protezione dei Dati Personali che riguardano sia la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Trattamento, sia la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico. L'efficacia di tali misure è oggetto di monitoraggio periodico.

Relativamente alle società che utilizzano sistemi informativi diversi da quelli in uso presso il Gruppo, sono assicurate misure per garantire la sicurezza, da utilizzi fraudolenti e da aggressioni esterne, dei dati e delle informazioni trattate attraverso il sistema informativo secondo quanto stabilito nelle Linee Guida di Gruppo del Sistema Informativo.

3.1.8 Conservazione e cancellazione dei Dati Personali

I Dati Personali sono 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 raccolti e trattati. Al venire meno di tali finalità, i Dati Personali devono essere resi non più riconducibili all'Interessato.

Il periodo di conservazione dei Dati Personali, in relazione alle finalità per cui gli stessi sono trattati, è determinato valutando in particolare i seguenti fattori:

- **criterio di necessità**: i Dati Personali sono conservati per l'arco di tempo necessario affinché le finalità di Trattamento per le quali i dati sono stati raccolti ed eventuali finalità strettamente connesse o derivanti da queste possano dirsi pienamente perseguite e soddisfatte;
- **obbligo di legge**: i Dati Personali sono conservati per l'arco di tempo necessario affinché possano ritenersi pienamente assolti gli obblighi normativi cui è soggetto il Titolare del Trattamento e almeno per il periodo richiesto dalla normativa stessa;
- **criterio di opportunità**: i Dati Personali sono conservati per l'arco di tempo necessario per il perseguimento di legittimi interessi del Titolare del Trattamento, laddove tale interesse non prevalga sui diritti e le libertà dei soggetti Interessati e la normativa di riferimento non specifichi un periodo di conservazione determinato.

3.1.9 Trattamento di dati personali per conto del Titolare da parte di Terzi

Il Trattamento di dati personali per conto del Titolare da parte di Terzo è sottoposto a specifiche prescrizioni normative affinché sia garantito un livello adeguato di protezione dei dati. In particolare, i Responsabili del Trattamento presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti derivanti dalla normativa di riferimento e garantisca la tutela dei diritti dell'Interessato.

I Trattamenti da parte di un responsabile del Trattamento sono disciplinati da apposito contratto o da altro atto giuridico (ad es. Data Protection Agreement), che vincoli il responsabile del Trattamento al Titolare del Trattamento e che dovrà contenere le informazioni di cui all'art.28, par.3 GDPR, la materia disciplinata e la durata del Trattamento, la natura e la finalità del Trattamento, il tipo di dati personali e le categorie di Interessati, nonché gli obblighi e i diritti delle parti.

Il modello di Data Protection Agreement adottato da BPER è previsto nei casi in cui la terza parte effettui un'attività di Trattamento di Dati Personali per conto di BPER.

3.1.10 Trasferimento transfrontaliero di Dati Personali

Il trasferimento di Dati Personali oggetto di un Trattamento verso un paese terzo o un'organizzazione internazionale, può avvenire unicamente in presenza di una decisione di adeguatezza da parte della Commissione Europea o con adeguate garanzie ai soggetti Interessati circa il livello di protezione dei dati e l'esercizio dei diritti previsti dalla normativa di riferimento.

Possono costituire adeguate garanzie:

- nell'ambito di un Gruppo imprenditoriale, norme vincolanti d'impresa, approvate dall'Autorità di Controllo

di riferimento;

- clausole contrattuali tipo, coerenti con il modello adottato dalla Commissione Europea, tra il soggetto esportatore dei Dati Personali e il soggetto importatore;
- codice di condotta approvato, unitamente all'impegno vincolante ed esecutivo da parte del Titolare del Trattamento o del Responsabile del Trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati;
- meccanismo di certificazione approvato, unitamente all'impegno vincolante ed esigibile da parte del Titolare del Trattamento o del Responsabile del Trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati.

3.1.11 Gestione delle richieste di esercizio dei diritti degli Interessati:

Le richieste di esercizio diritti da parte degli Interessati sono gestite nel rispetto del principio di trasparenza, fornendo un riscontro al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste, previa adeguata comunicazione all'Interessato di tale proroga, e dei motivi del ritardo.

Qualora vi siano ragionevoli dubbi circa l'identità del soggetto richiedente, è possibile richiedere ulteriori informazioni necessarie per confermare l'identità dell'Interessato.

Le richieste ricevute e il relativo stato di avanzamento sono tracciate in un apposito registro, anche con l'obiettivo di monitorare il rispetto dei tempi di risposta previsti dalla normativa di riferimento.

3.1.12 Gestione degli eventi di Data Breach

Eventuali eventi di violazione dei Dati Personali sono notificati all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare del trattamento ne viene a conoscenza, a meno che sia improbabile che la violazione dei Dati Personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Inoltre, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento comunica la violazione all'Interessato senza ingiustificato ritardo, descrivendo con un linguaggio semplice e chiaro la natura della violazione dei Dati Personali e indicando almeno le informazioni richieste dalla Normativa di riferimento.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

- il Titolare del Trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai Dati Personali oggetto della violazione, in particolare quelle destinate a rendere i Dati Personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- il Titolare del Trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, è consentita una comunicazione pubblica o una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

Gli eventi di Data Breach occorsi sono tracciati e documentati in un apposito registro dei Data Breach.

Al fine di mantenere un approccio uniforme a livello di Gruppo, la Capogruppo ha definito un approccio metodologico comune e le relative metriche di valutazione per la determinazione del livello di impatto dei Data Breach.

4 Governo del rischio di non conformità alla normativa in materia di Protezione dei dati personali

4.1 Definizione del rischio

Il Rischio di non conformità alla normativa in materia di protezione dei Dati Personali è il rischio di condurre

attività di Trattamento di Dati Personali in violazione della normativa di riferimento e dei principi fondamentali definiti nel paragrafo 3.1 e, conseguentemente, di causare impatti negativi per i soggetti Interessati nonché di incorrere in sanzioni amministrative, illeciti penali, danni reputazionali o misure prescrittive che limitino lo svolgimento delle regolari operazioni di Trattamento.

4.2 Governo del rischio

Le decisioni strategiche a livello di Gruppo in materia di governo del rischio sono rimesse agli organi aziendali della Capogruppo. Le scelte effettuate tengono conto delle specifiche operatività e dei connessi profili di rischio di ciascuna società componente il Gruppo in modo da realizzare una politica di gestione dei rischi integrata e coerente.

A tale proposito il Gruppo BPER si è dotato di un modello di governo dei rischi in base al quale ciascun rischio è assunto a livello decentrato ma sotto il coordinamento e l'indirizzo della Capogruppo mentre le attività di gestione del rischio sono volte in via accentrata dalla Capogruppo.

BPER Banca, in qualità di Capogruppo, è responsabile nel definire le linee di indirizzo del governo del rischio di non conformità per l'intero Gruppo Bancario.

L'attuazione degli indirizzi formulati dalla Capogruppo avviene secondo principi di gradualità e proporzionalità in funzione delle specificità delle diverse società appartenenti al Gruppo e rientranti nel perimetro.

4.3 Propensione al rischio

Il Gruppo BPER considera come principi fondamentali nello svolgimento della propria attività il rispetto delle norme e la correttezza formale e sostanziale nell'operatività. Ogni deviazione da tali principi viene ritenuta inaccettabile.

Il Gruppo ritiene pertanto necessario che l'operatività sia improntata al rispetto formale e sostanziale delle norme vigenti.

I presidi al fine della conformità alla Normativa in materia di protezione dei dati Personali sono adottati dal Titolare del Trattamento, nel rispetto del principio di accountability, secondo un approccio basato sul rischio.

4.4 Limiti di esposizione e operativi

Tale paragrafo non è valorizzato in quanto il rischio disciplinato nella presente policy rientra tra i rischi non misurabili.

4.5 Assunzione e mitigazione

Si rinvia alla Policy di Gruppo per il governo del rischio di non conformità.

5 Ruoli e responsabilità in materia di Protezione dei Dati Personali

Il Consiglio di Amministrazione della Capogruppo ha adottato un modello organizzativo di Gruppo per garantire l'effettiva gestione delle attività sopra dettagliate, ai fini della protezione dei Dati Personali e dei diritti degli Interessati.

l Titolare del Trattamento dei dati di ciascuna Società è tenuto a impartire istruzioni su come i Soggetti Autorizzati sono tenuti al trattamento dei Dati Personali nell'ambito dell'attività lavorativa.

Tale modello, prevede in particolare le seguenti figure fondamentali:

- un **Delegato privacy** in BPER e in ciascuna Società del Gruppo Bper a perimetro, individuato nell'Amministratore delegato (ove presente) o nel Direttore generale dal Consiglio di Amministrazione di ciascuna società in qualità di Titolare del Trattamento, con il compito di attuare, in piena autonomia operativa e con facoltà decisionale anche sotto il profilo della capacità di spesa, i provvedimenti e le misure tecniche e organizzative richieste dalla normativa di riferimento, con conseguente assunzione di ogni relativa responsabilità, per garantire ed essere in grado di dimostrare che il Trattamento dei

Dati Personali è effettuato conformemente alla normativa vigente. Il Delegato esercita le funzioni tramite i poteri decisionali, organizzativi e di disposizione, sia ordinari che straordinari, ad esso attribuiti, anche sotto il profilo della capacità di spesa, con facoltà di sub-delega degli stessi, nonché gli inerenti poteri rappresentativi. Il conferimento delle citate deleghe lascia, tuttavia, in carico al Titolare/Consiglio di Amministrazione le responsabilità amministrative, le azioni risarcitorie, gli accertamenti e i provvedimenti delle Autorità di Controllo e le responsabilità civili e penali non riconducibili al Delegato.

- un unico **DPO** per le Società del Gruppo BPER a perimetro, designato dal Consiglio di Amministrazione di ciascuna società in qualità di Titolare del Trattamento, cui spettano le funzioni e i compiti previsti dall'art. 39 del GDPR tra cui quelli di informare e fornire consulenza in merito agli obblighi derivanti dalla normativa di riferimento, sorvegliarne l'osservanza, cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al Trattamento.

5.1 Ruoli e responsabilità previsti nel modello organizzativo di Gruppo

- <u>di Capogruppo</u>:

Organo Aziendale / U.O.	**Descrizione Ruoli e Responsabilità**
Delegato Privacy	Attua, in piena autonomia operativa e con facoltà decisionale anche sotto il profilo della capacità di spesa, le misure tecniche e organizzative adeguate a norma degli articoli 24 e 32 del Regolamento, con conseguente assunzione di ogni relativa responsabilità, per garantire ed essere in grado di dimostrare che il Trattamento dei Dati Personali è effettuato conformemente alla normativa vigente
Data Protection Officer (DPO)	Effettua i compiti e le funzioni previste dall'art. 39 del GDPR tra cui quelli di informare e fornire consulenza in merito agli obblighi derivanti dalla normativa di riferimento, sorvegliarne l'osservanza, cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al Trattamento;

- <u>delle altre società del Gruppo</u>:

Organo Aziendale / U.O.	**Descrizione Ruoli e Responsabilità**
Delegato Privacy	Medesime responsabilità previste per la Capogruppo.
Data Protection Officer (DPO)	Medesime responsabilità previste per la Capogruppo.

6 Flussi informativi

Con cadenza almeno annuale, il DPO relaziona il Delegato Privacy circa l'efficacia dei presidi adottati in materia di protezione dei dati ed eventuali rischi che possano impattare in modo significativo le operazioni di trattamento condotte e risultare nel mancato rispetto dei principi di protezione dei dati o in situazioni di non conformità rispetto alla normativa di riferimento.

Per la declinazione dei **"flussi orizzontali"** ovvero quelli scambiati fra le funzioni di controllo (aziendali e

non) e dei **"flussi verticali"** ovvero quelli scambiati fra le funzioni di controllo (aziendali e non) e gli Organi aziendali, si rimanda alla fonte normativa "Flussi informativi funzioni di controllo – Organi aziendali".

7 Allegati

7.1 Storico degli aggiornamenti

Si riporta di seguito lo storico degli aggiornamenti:

Versione	Data di approvazione	Nr. Direttiva	Sintesi delle modifiche
1.0	12/04/2016	19/2016	• Emanazione
2.0	20/12/2018	10/2019	• Recepimento delle modifiche normative ex Regolamento UE 2016/679 – GDPR • Definizione del ruolo di Responsabile della Protezione dei Dati (Data Protection Officer – DPO) • Introduzione di un nuovo modello organizzativo nelle società appartenenti al Gruppo • Formalizzazione del processo "adempimenti normativi Privacy e Data Protection"

7.2 Contesto normativo di riferimento

Normativa in materia di protezione dei Dati Personali:

Si riporta di seguito il quadro delle principali fonti di normativa esterna applicabili all'ambito della protezione dei Dati Personali e di riferimento per il Gruppo Bper:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati (Regolamento Generale sulla protezione dei dati – GDPR);
- D.lgs. 101 del 10 agosto 2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- Provvedimenti del Garante Privacy (comprensivi sia di quelli di natura generale che di quelli specifici riguardanti il settore bancario);
- Codici di Condotta in materia di protezione dei dati personali, approvati dall'Autorità di Controllo Competente.
- Linee Guida e raccomandazioni del Working Party art. 29 (WP29), il gruppo di lavoro europeo indipendente che, fino al 25 maggio del 2018 (entrata in vigore del GDPR) aveva lo scopo di occuparsi di questioni relative alla protezione della vita privata e dei Dati Personali;
- Linee Guida e raccomandazioni dell'European Data Protection Board (EDPB), l'organismo europeo indipendente, che, a far data dal 25 maggio 2018, ha sostituito il Working Party 29 e contribuisce

all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità dell'UE per la protezione dei dati.

Normativa interna:

- Codice Etico;
- Linee guida Governo di Gruppo;
- Policy – Sistema dei controlli Interni;
- Policy di Gruppo per il governo del rischio di non conformità.