Gruppo BPER

Policy in materia di protezione dei dati personali

Modena, 07/05/2025

Versione 4.0

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. Il Gruppo BPER ha 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 vigente, il documento sarà oggetto di revisione e aggiornato ogniqualvolta intervengano modifiche rilevanti del contesto interno o esterno di riferimento.

Rispetto alla precedente edizione, la presente 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, la presente edizione della Policy ha – tra l'altro - introdotto:

i) le valutazioni condotte nell'ambito dell'intelligenza artificiale, al fine di valutare la conformità dei modelli di intelligenza artificiale alla normativa in materia di protezione dei dati personali;
ii) il reporting periodico dalle Società del Gruppo verso il DPO, funzionale a rendicontare quest'ultimo sulle attività o, comunque, sugli eventi che rilevano sotto il profilo della tutela e della protezione dei dati personali;
iii) un iter di escalation atto a portare una decisione al livello gerarchico superiore al fine di gestire eventuali rischi di non conformità alla normativa in materia di data protection.

Redattore:

Ufficio Group Data Protection

Approvatore:

CdA

Destinatari del documento:

Banche		**Società**					
Italiane		Strumentali		Finanziarie		Altre società controllate*	
X	Bper	X	MO Terminal	-	Di Credito		Adras
X	Bibanca	X	Bper Real Estate	X	Bper Factor		Arca Holding
X	Banco di Sardegna	X	Bper Trust Company	X	Sardaleasing		Commerciale Piccapietra
X	Banca Cesare Ponti			X	Finitalia		St. Anna Golf
Estere				-	Non di Credito		St. Anna Gestione Golf
	Bper Bank Luxembourg			X	Estense C. Bond		Annia
				X	Estense C.B.CPT		
					Arca Fondi SGR		
				X	Carige C. Bond		
				X	Lanterna Finance		
				X	Lanterna Mortgage		

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 e/o dalle norme 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'art. 51 del GDPR. In Italia l'autorità di controllo è il Garante Privacy.
- **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 o Dati:** 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, 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/Direttore Generale di ciascuna società del Gruppo, 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 artt. 24 e 32 del GDPR, 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'art. 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 del GDPR).
- **GDPR (**o **Regolamento):** 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 (General Data Protection Regulation).
- **Incaricato o Persona Autorizzata:** 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 nell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, e, più in generale, tutti coloro che trattano Dati Personali di clienti, dipendenti e fornitori o, comunque, Dati di titolarità del Titolare sotto la diretta autorità di

quest'ultimo

- **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.
- **Privacy Contact**: nelle Banche e nelle Società del Gruppo BPER è la figura incaricata di svolgere compiti operativi, informativi e di raccordo a supporto dell'Ufficio Group Data Protection e del DPO del Gruppo, con il quale opera a stretto contatto.
- **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 (non stabiliti nel territorio dell'Unione) per iscritto ai sensi dell'art. 27 del 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.
- **Sistemi di Intelligenza Artificiale**: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.
- **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 (accountability) che il Trattamento

è effettuato nel rispetto della Normativa in materia di Protezione dei Dati Personali.

3.1 Principi applicabili al Trattamento dei Dati Personali

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 (c.d. basi giuridiche):

- 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.

Nello stabilire la specifica base giuridica per un determinato Trattamento, il Titolare deve tenere conto delle finalità perseguite con il Trattamento stesso e distinguere la base giuridica individuata in relazione ad un singolo Trattamento rispetto alle basi giuridiche impiegate per altri eventuali ed ulteriori Trattamenti.

Al venire meno della base giuridica, il Trattamento deve cessare, fuorché nel caso in cui il Titolare sia in grado di proseguire il Trattamento in maniera lecita impiegando una diversa base giuridica.

Il Trattamento di Dati Particolari è invece vietato, salvo che sussista almeno una delle condizioni di cui all'art. 9, par. 2, del GDPR.

Si precisa che l'individuazione di una appropriata base giuridica non è sufficiente, di per sé, a conferire liceità a un Trattamento di Dati Personali: il Titolare è invero tenuto a conformarsi anche a tutte le ulteriori disposizioni rilevanti in materia.

Quanto al profilo della correttezza, esso fa riferimento alle concrete modalità cui deve essere improntato il rapporto tra Titolare e Interessati. In virtù di tale principio, il Titolare deve astenersi dal porre in essere comportamenti generalmente scorretti nei rapporti intercorrenti con gli Interessati stessi.

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 relative al Trattamento di cui agli artt. 13 e 14 del GDPR e le comunicazioni di cui agli artt. da 15 a 22 e all'art. 34:

- in forma concisa trasparente, intelligibile e facilmente accessibile;
- con un linguaggio semplice e chiaro;
- per iscritto o con altri mezzi anche, se del caso, elettronici;
- generalmente in via gratuita.

Il Titolare del Trattamento, inoltre, è tenuto ad agevolare l'esercizio dei diritti dell'Interessato ai sensi degli artt. 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'art. 33, par. 3, lett. b), c) e d) del GDPR.

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.

Le finalità sono “determinate” quando il perimetro del Trattamento è ben definito da parte del Titolare, che è pertanto tenuto a verificare accuratamente gli scopi specifici per i quali intende trattare i Dati Personali.

Le finalità sono “esplicite” quando sono rese manifeste all’esterno della sfera del Titolare del Trattamento e delineate in modo chiaro e privo di ambiguità nei confronti degli Interessati.

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.

Prima di raccogliere e trattare Dati Personali, il Titolare del Trattamento è tenuto a svolgere una valutazione preliminare in termini di minimizzazione, muovendo dalle specifiche finalità cui ogni Trattamento è preordinato. In particolare, devono escludersi tutti quei Dati Personali e quelle forme di Trattamento che, all’esito della valutazione, risultino non strettamente necessari al perseguimento della finalità esaminata.

Più in dettaglio, il principio di minimizzazione è attuato sia al momento di determinare i mezzi del Trattamento, sia all’atto del Trattamento e, in ogni caso 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.

Integrità e riservatezza

I Dati Personali, per l’intero ciclo di vita, sono trattati in maniera da garantirne un’adeguata sicurezza. È dunque onere del Titolare del Trattamento l’individuazione e l’attuazione di misure di sicurezza tecniche e organizzative adeguate ai Trattamenti svolti, nonché al rischio che essi possono comportare per i diritti e le libertà delle persone fisiche.

In particolare, devono essere adottate misure tali da preservare i Dati Personali da rischi quali i Trattamenti non autorizzati o illeciti, la perdita e distruzione dei Dati o il danno accidentale.

3.2 Presidi in materia di protezione dei Dati Personali

Il principio di responsabilizzazione ("accountability") prevede che il Titolare del Trattamento sia, da un lato, responsabile per il rispetto della Normativa applicabile in materia di protezione dei Dati Personali e, dall'altro, in grado di dimostrare attivamente e in concreto la propria conformità.

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 suddetto principio di responsabilizzazione, 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.

3.2.1 Trattamento di Dati Particolari e Dati Giudiziari

Il Trattamento di 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.

3.2.2 Nomina di Persone Autorizzate

I soggetti che, nello svolgimento delle attività di propria competenza, effettuano Trattamenti di Dati Personali sono designati Persone Autorizzate al Trattamento. La designazione avviene tramite apposito documento di nomina con cui il Titolare impartisce alla Persona Autorizzata le istruzioni, riferibili all’ambito di assegnazione del soggetto, cui attenersi nel Trattamento di Dati Personali.

Inoltre, al fine di aumentare la consapevolezza delle Persone Autorizzate 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 sulla Normativa in materia di protezione dei Dati Personali.

3.2.3 Informativa all’Interessato

L’informativa all’Interessato contiene, di fatto, le informazioni richieste dalla Normativa in materia di protezione dei Dati Personali, con particolare riferimento agli artt. 13 e 14 del GDPR.

Se i Dati Personali sono raccolti presso l'Interessato, l’informativa è fornita nel momento in cui i Dati Personali sono ottenuti.

Se i Dati Personali sono raccolti presso soggetti terzi, l’informativa è fornita:

- entro un termine ragionevole dall'ottenimento dei Dati Personali e comunque, al più tardi, entro un mese dall’ottenimento degli stessi;
- se i Dati Personali sono destinati alla comunicazione con l'Interessato, al più tardi al momento della prima comunicazione con lo stesso;
- nel caso sia prevista la comunicazione ad altro Destinatario, non oltre la prima comunicazione dei Dati personali.

L’informativa deve essere data in un formato chiaro, facilmente intellegibile e comprensibile dall’Interessato, e contenere tutte le informazioni richieste dalla Normativa in materia di protezione dei Dati Personali, 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 DPO;
- le finalità del Trattamento dei Dati Personali e il presupposto di liceità del Trattamento (base giuridica);
- 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;
- il legittimo interesse perseguito 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 (ai sensi dell’art. 6, par. 1, lett. a) oppure dell’art. 9, par. 2, lett. a) del GDPR);
- gli eventuali Destinatari o le eventuali categorie di Destinatari dei Dati Personali;
- l'intenzione di trasferire Dati Personali a un Destinatario situato al di fuori dello Spazio Economico Europeo 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;
- il diritto di proporre reclamo a un'Autorità di Controllo.

3.2.4 Trattamenti basati sul Consenso dell'Interessato

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.

3.2.5 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 la prevalenza dell'interesse legittimo rispetto ai diritti e alle libertà fondamentali degli Interessati i cui Dati Personali sono trattati. Tale bilanciamento di interessi (c.d. *Legitimate Interest Assessment LIA*), che consiste in un test comparativo, deve essere condotto tenendo 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 sugli interessi del Titolare, per lo svolgimento del Trattamento è necessario identificare un differente presupposto di liceità, valutando in particolare la possibilità di acquisire un consenso esplicito dell'Interessato.

3.2.6 Tenuta ed aggiornamento del registro delle attività di Trattamento

Il Registro dei Trattamenti è un documento di censimento e analisi contenente un'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 in materia di protezione dei Dati Personali, in particolare dall'art. 30 del GDPR, tra cui:

- il nome e i dati di contatto del Titolare del Trattamento e, ove applicabile, del Contitolare del Trattamento e/o del Rappresentante;
- la denominazione e i dati di contatto 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.

3.2.7 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 i diritti e le libertà delle persone fisiche, è necessario, prima di procedere al Trattamento, condurre una valutazione di impatto dei Trattamenti sulla protezione dei Dati Personali (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 DPIA è condotta preliminarmente all'avvio del Trattamento e revisionata al ricorrerne dei presupposti. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi analoghi.

Nell'ipotesi in cui dalla DPIA risulti un elevato rischio per gli Interessati 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.

3.2.8 Adozione di adeguate misure a protezione dei dati

Per l'intera durata del relativo ciclo di vita del Trattamento, 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 BPER 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 non allineate informaticamente, 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 nella Policy del Sistema Informativo.

3.2.9 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.

3.2.10 Trattamento di Dati Personali per conto del Titolare da parte di Terzi

Il Trattamento di Dati Personali di titolarità del Titolare da parte di un Terzo è sottoposto a specifiche prescrizioni normative affinché sia garantito un livello adeguato di protezione degli stessi. In particolare, i Responsabili del Trattamento devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti derivanti dalla Normativa in materia di protezione dei Dati Personali e garantisca la tutela dei diritti dell'Interessato.

I Trattamenti svolti da un Responsabile del Trattamento sono disciplinati da apposito contratto o da altro atto giuridico (ad es. *Data Protection Agreement DPA*), che vincoli il Responsabile del Trattamento al Titolare del Trattamento e che dovrà riportare le informazioni di cui all'art. 28, par. 3, del GDPR, quali 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, nella disponibilità dei competenti Uffici del Gruppo BPER, è da utilizzarsi ogniqualvolta il Terzo fornitore della Banca si trovi a trattare Dati Personali di titolarità di quest'ultima al fine di erogare uno specifico servizio.

3.2.11 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, resa dalla Commissione Europea, relativamente al livello di protezione garantito dalla normativa del paese terzo o dalla organizzazione; ovvero – in assenza di simile decisione – qualora il terzo abbia fornito adeguate garanzie ai soggetti Interessati circa il livello di protezione dei Dati e l'esercizio dei diritti previsti dalla normativa di riferimento. In ogni caso, il trasferimento deve avvenire nel rispetto delle raccomandazioni fornite dall'Autorità di Controllo.

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.

La valutazione circa le adeguate garanzie prestate dal Destinatario di Dati Personali che si trovi al di fuori dello Spazio Economico Europeo può avvenire previa esecuzione di apposita valutazione di impatto del trasferimento per ciascuna attività di Trattamento che preveda il trasferimento dei Dati (c.d. Transfer Impact Assessment - TIA).

3.1.2 Gestione delle richieste di esercizio dei diritti degli Interessati:

Le richieste di esercizio dei diritti di cui agli artt. 15-22 del GDPR degli Interessati sono agevolate da parte del Titolare del Trattamento e sono gestite nel rispetto del principio di trasparenza, fornendo agli Interessati le

informazioni relative all'azione intrapresa senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste ricevute, previa adeguata comunicazione all'Interessato, entro i trenta giorni dal ricevimento della richiesta, della volontà di esercitare 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 nella gestione delle stesse sono tracciate in un apposito registro, anche con l'obiettivo di monitorare il rispetto dei tempi di risposta previsti dalla normativa di riferimento nel rispetto del principio di *accountability*.

3.2.12 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 coinvolte.

Qualora la notifica all'Autorità di Controllo sia effettuata oltre il termine di 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 coinvolte, 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 in materia di protezione dei Dati Personali.

Non è richiesta la comunicazione della violazione occorsa 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.

3.2.13 Valutazione di Sistemi di Intelligenza Artificiale

Al fine di garantire la tutela e la protezione dei Dati Personali anche nell'ambito della progettazione, dello sviluppo, dell'addestramento, nonché dell'utilizzo di Sistemi di Intelligenza Artificiale, è valutata, in ottica di *data protection by design*, la conformità degli stessi alla Normativa in materia di protezione dei Dati Personali.

Per maggiori informazioni in merito alla valutazione dei Sistemi di Intelligenza Artificiale, si rimanda al *Regolamento del Processo di Etica e Governo dei Sistemi di Intelligenza Artificiale*.

3.3 Governo del rischio di non conformità alla normativa in materia di Protezione dei Dati Personali

3.3.1 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 stessa e dei principi fondamentali definiti nel paragrafo 3.1 e nel paragrafo 3.2 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.

3.3.2 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 svolte 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.

3.3.3 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 BPER 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.

3.3.4 Limiti di esposizione e operativi

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

3.3.5 Assunzione e mitigazione

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

3.4 Iter di escalation

Qualora a livello di progetto, iniziativa, prodotto, servizio o altro tavolo sia rilevato un rischio di non conformità alla Normativa in materia di protezione dei Dati Personali, la cui eliminazione o mitigazione non risulti praticabile a causa, a titolo esemplificativo e non esaustivo, di contrapposte esigenze o istanze di cui sono portatrici le funzioni aziendali competenti, deve osservarsi l'iter di escalation di seguito delineato, al fine di addivenire ad una gestione tempestiva e ponderata della questione insorta.

Il DPO informa tempestivamente il Chief Compliance Officer per le opportune valutazioni.

Il Chief Compliance Officer, in caso di persistenza o particolare rilevanza della questione insorta, nonché di altra circostanza a suo insindacabile giudizio ritenuta meritevole di attenzione, ne dà a sua volta avviso al proprio organo gerarchicamente superiore che riveste il ruolo di Delegato privacy.

3.5 Modello organizzativo 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.

Il 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, dal Consiglio di Amministrazione di ciascuna società in qualità di Titolare del Trattamento, nell'Amministratore delegato (ove presente) o nel Direttore generale, 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.
- un **Privacy Contact** per ciascuna delle altre Società del Gruppo BPER, designato in seno a ciascuna di esse, incaricato di svolgere compiti operativi, informativi e di raccordo a supporto dell'Ufficio Group Data Protection e del DPO del Gruppo, nonché ogni ulteriore compito previsto dalle fonti di normativa interna.

3.6 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".

Al fine di garantire una costante interazione tra il DPO e le Società del Gruppo BPER, nonché di consentire al DPO stesso di monitorare il corretto adempimento, da parte delle citate società, dei principali obblighi in materia di protezione dei Dati Personali, è previsto un sistema di reporting periodico.

Il sistema di reporting periodico consiste in un flusso informativo, da parte dei Privacy Contact verso il DPO, avente ad oggetto gli esiti e gli aggiornamenti di attività che rilevano sotto il profilo della protezione dei Dati Personali (quali, a titolo esemplificativo e non esaustivo, informazioni inerenti a Data Breach, variazioni apportate al Registro delle attività di Trattamento, DPIA, LIA e TIA condotte, richieste di esercizio dei diritti degli Interessati).

Il reporting viene effettuato mediante compilazione di apposito template condiviso con il DPO, aggiornato conformemente al contesto normativo interno ed esterno tempo per tempo vigente.

Il reporting è trasmesso dai Privacy Contact al DPO con cadenza trimestrale, entro il 15 del mese successivo al trimestre di riferimento.

Unitamente al reporting relativo al secondo trimestre dell'anno (reporting al 30 giugno), i Privacy Contact trasmettono al DPO anche un reporting semestrale.

Unitamente al reporting relativo al quarto trimestre (reporting al 31 dicembre), i Privacy Contact trasmettono al DPO anche un reporting relativo all'intera annualità, nonché il Registro dei Trattamenti aggiornato alla medesima data.

Quanto sopra illustrato non esime i Privacy Contact dall'informare senza indugio il DPO al verificarsi di eventi rilevanti sotto il profilo data protection che siano ritenuti meritevoli di particolare attenzione in ragione delle loro peculiarità e/o altre caratteristiche.

3.7 Ruoli e responsabilità

di Capogruppo:

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 artt. 24 e 32 del GDPR, 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

- delle altre società del Gruppo:

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.
Privacy Contact	Supporta ed eventualmente chiede consulenza al DPO nello svolgimento dei propri compiti operativi e di raccordo, conformemente a quanto previsto dalla normativa interna, ivi compresa l'attivazione dei previsti flussi informativi.

4 Allegati

4.1 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"
3.0	24/12/2022	89/2922	• Definizione più puntuale dei requisiti e delle misure nonché dei principi generali; • Introduzione della necessità di condurre un Legitimate Interest Assessment per i trattamenti di dati personali fondati sul legittimo interesse;

4.2 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. 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali e ss.mm.ii;
- D.lgs. 101 del 10 agosto 2018 recante "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;
- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

Normativa interna:

- Codice Etico;
- Linee guida Governo di Gruppo;
- Policy – Sistema dei controlli Interni;
- Flussi Informativi - Funzioni di Controllo - Organi Aziendali;
- Policy di Gruppo per il governo del rischio di non conformità;