# Policy di Gruppo del governo del rischio di non conformità alla normativa in materia di Protezione dei dati personali

Modena, */2018*

Versione XXX (inserire la versione)

**INDICE**

# 1 Sintesi principali tematiche trattate / modifiche apportate

Il documento descrive il modello adottato dal Gruppo BPER[1] per assicurare la conformità del proprio operato e delle proprie procedure alla normativa in materia di "protezione dei dati personali"[2].

L'aggiornamento, rispetto alla precedente versione,

- recepisce:
  - gli aggiornamenti intervenuti nella normativa esterna, in particolare a seguito della entrata in vigore del Regolamento Generale sulla Protezione dei dati (Regolamento (UE)2016/679, GDPR)
  - le modifiche organizzative intervenute, in particolare a seguito della istituzione della figura del Responsabile della Protezione dei Dati/DPO del Gruppo
- introduce:
  - il nuovo modello organizzativo in tema di "protezione dei dati personali" del Gruppo BPER
  - modifiche al processo gestione del rischio di non conformità alla specifica normativa, con particolare riferimento alla declinazione del Processo "adempimenti normativi Privacy e Data Protection" e delle conseguenti attività e responsabilità in capo a ciascuna Società del Gruppo sia in qualità di Titolare del trattamento, sia, eventualmente, in qualità di Responsabile del trattamento

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 | Xx/xx/2018 | Xx/2018 | • Recepimento delle modifiche normative ex Regolamento (UE) 2016/679 – GDPR<br>• Definizione del ruolo di Responsabile della Protezione dei Dati (Data Protection Officer – DPO)<br>• Introduzione di un nuovo modello organizzativo nelle società appartenenti al Gruppo<br>• Formalizzazione del processo "adempimenti normativi Privacy e Data Protection" |

[1] Nel seguito anche "Gruppo" o "BPER Gruppo.

[2] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 – "Regolamento Generale sulla Protezione dei Dati, nel seguito anche Regolamento o GDPR.

# 2 Aspetti generali

## 2.1 Obiettivo della Policy

La Policy descrive gli indirizzi che BPER Banca[3], in qualità di Capogruppo, ha definito per le Società del Gruppo al fine di assicurare la protezione dei dati personali nel corso delle proprie attività, in conformità con regole e principi previsti dalla normativa di riferimento e in base alla "Policy di Gruppo per il Governo del rischio di non conformità".

Con riferimento alle società controllate non facenti parte del Gruppo civilistico la Capogruppo, nella sua funzione di indirizzo e coordinamento, valuta caso per caso l'assetto del sistema dei presidi in materia privacy.

## 2.2 Destinatari del documento

Banche italiane, Società finanziarie di credito, Optima Sim e Società, del Gruppo.

## 2.3 Gestione del documento

Le responsabilità delle fasi del processo di gestione del documento sono declinate nel prospetto seguente

| Capogruppo | | | | | | | | | Società del Gruppo |
|---|---|---|---|---|---|---|---|---|---|
| **Iniziativa** | **Autorizzazione a procedere** | **Redazione** | **Parere di coerenza** | **Parere di conformità** | **Validazione** | **Approvazione** | **Divulgazione** | **Archiviazione** | **Recepimento** |
| Ufficio Privacy e Data protection | Responsabile Protezione Dati / DPO | Ufficio Privacy e Data protection | Ufficio Assetti Organizzativi e Normativa | Non previsto | Comitato Controlli e Rischi | Consiglio di Amministrazione | Ufficio Coordinamento Organi Societari di Gruppo | Ufficio Assetti Organizzativi e Normativa | CdA |

## 2.4 Gestione delle eccezioni

Ogni eccezione alla Policy, nella Capogruppo e nelle Società del Gruppo, deve essere preventivamente sottoposta, all'Amministratore Delegato della Capogruppo che ne darà informativa al Consiglio di Amministrazione della Capogruppo, proponendo gli eventuali interventi di adeguamento corredati delle necessarie motivazioni.

## 2.5 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:

- **Amministratore di sistema**[4]**:** in ambito informatico, figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti; vengono però considerate tali

[3] Da questo punto in poi anche BPER, BPER Banca o Capogruppo.

[4] Da questo punto in poi anche AdS. "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" (G.U. n. 300 del 24 dicembre 2008) e "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento – 25 giugno 2009" (in G.U. n. 149 del 30 giugno 2009) del Garante.

anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi

- **Archivio:** qualsiasi insieme strutturato di Dati Personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

- **Aree Sensibili:** sono quei luoghi fisici o della Rete Aziendale in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio.

- **Autorità di Controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;

- **Autorizzazione al trattamento dei Dati Personali**: atto con il quale il Titolare / la Società autorizza un soggetto, nello svolgimento della propria mansione lavorativa, a svolgere operazioni di trattamento per specifiche tipologie di dati personali per proprio conto, in virtù appunto delle mansioni svolte. Infatti, l'art. 29 del GDPR prevede che le operazioni di Trattamento possono essere svolte solo da soggetti "autorizzati" che operano sotto la diretta autorità del titolare o del responsabile del Trattamento; tali soggetti, devono attenersi, nell'effettuare le attività di Trattamento, alle istruzioni loro impartite e la loro designazione, effettuata per iscritto, deve individuare l'ambito del Trattamento consentito;

- **Consenso dell'Interessato** o **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 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 Comuni:** sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;

- **Dati Genetici:** i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- **Dati Giudiziari:** Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

- **Dati Particolari:** Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

- **Dati relativi alla Salute:** i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- **Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**Interessato**"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- **Destinatario/i**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, 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 non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;

- **Device Fissi**: si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;

- **Device Mobili**: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet, pc portatili e smartphone utilizzati dalla Persone Autorizzate per uso professionale;

- **DPO** o **Data Protection Officer**: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;

- **GDPR (**o **Regolamento):** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679;

- **Gruppo Imprenditoriale**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

- **Incaricato/i o Persona/e Autorizzata/e:** si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. 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, compresi gli indirizzi di posta elettronica.

- **Limitazione Di Trattamento:** il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro;

- **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 analogo significativamente sulla sua persona;

- **Profilazione:** qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere 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 più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative 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, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del 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; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato;

- **Rete Aziendale:** rappresenta il perimetro digitale della Società, possibilmente contenente Dati Personali e/o informazioni riservate, comprensivo dei dispositivi hardware/software sia per la gestione dei servizi interni (es. switch, LAN, Wi-Fi) che dei collegamenti da o verso l'esterno (es. boundary router, SSH, VPN).

- **Strumenti Aziendali**: l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dalla Società alle Persone Autorizzate al fine di svolgere le proprie mansioni;

- **Strumenti Personali**: i Device Mobili di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale;

- **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** o **Trattato/Trattati:** 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;

- **Trattamento Transfrontaliero:** a) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del Trattamento o Responsabile del Trattamento nell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro;

- **Violazione Dei Dati Personali** ovvero **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 Contesto normativo di riferimento

**Normativa esterna**

- 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)”
- Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti (Provv. Garante Privacy n.8, 16 novembre 2004)

**Normativa interna**

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

# 4 Metodologie e Regole

Il Consiglio di Amministrazione della Capogruppo definisce indirizzi e regole uniformi per le Società del Gruppo per il rispetto della conformità alla normativa in parola, consapevole che l'attività di prevenzione dei rischi favorisce ed integra i presidi e i presupposti per una sana e prudente gestione delle singole entità e del Gruppo stesso.

In base alla manifestazione del rischio di non conformità alla normativa per la protezione dei dati personali, secondo il principio di *accountability* e nel rispetto delle previsioni della normativa in materia, sono stati costituiti appositi presidi nell'ambito delle seguenti attività:

- **tenuta e gestione del Registro delle Attività di Trattamento**: in linea a quanto disciplinato dall'art. 30 del GDPR, il Data Dictionary del Registro, ovvero il tracciato dati che rappresenta il patrimonio informativo di riferimento per il Registro, è stato predisposto sulla base di una interpretazione complessiva e sistematica del disposto normativo con l'obiettivo di produrre un modello di Registro idoneo a prevedere possibili evoluzioni future sia del Perimetro di applicabilità della normativa privacy, che possono determinare esigenze di registrazione di ulteriori informazioni a oggi non applicabili al contesto ma previste dal disposto normativo, sia del Modello di gestione della privacy o di informatizzazione del processo.
- **analisi di impatto sui trattamenti di dati personali – PIA/DPIA**: metodologia per valutare l'impatto sui diritti e le libertà delle persone fisiche di un progetto, servizio, applicazione, programma, prodotto o qualsiasi altra iniziativa che implichi il trattamento di dati personali che presenta alti rischi per i suddetti diritti e libertà delle persone fisiche e, dopo aver consultato tutti i terzi coinvolti nel trattamento dei dati e il DPO, prendere le misure necessarie per evitare o minimizzare l'impatto negativo. Si tratta di un processo continuo che deve iniziare nella fase più preliminare possibile del progetto, servizio, applicazione, programma, prodotto o iniziativa, quando, sia ancora possibile influenzarne il risultato, in modo tale da garantire la privacy by design.
- **gestione e comunicazione di DATA BREACH:** i sistemi di monitoraggio interni[5] mirano ad identificare eventi che possono comportare potenziali Data Breach relativi ai dati personali all'interno della Capogruppo. Il personale interno e i collaboratori hanno il compito di segnalare gli eventi potenzialmente rilevanti per la sicurezza dei dati personali di cui siano testimoni diretti o di cui siano venuti a conoscenza tramite segnalazioni di clienti o di terzi, coinvolgendo l'Ufficio Privacy e Data protection. I Fornitori in qualità di Responsabili esterni hanno il compito di segnalare gli eventi rilevanti per la sicurezza dei dati personali come disciplinato nel Privacy Agreement
- **gestione del rapporto con dipendenti e assimilabili:** in tutte le fasi del rapporto di lavoro, con riguardo alla formazione e alle istruzioni relative al trattamento dei dati personali, ai profili abilitativi al sistema informativo e all'utilizzo degli strumenti IT, alla circolazione delle informazioni e tracciamento delle operazioni bancarie, all'operatività degli amministratori di sistema
- **gestione del rapporto con i clienti:** con riguardo all'instaurazione del rapporto, alla consultazione dei sistemi di informazione creditizia (SIC), alla registrazione delle telefonate nella prestazione dei servizi di investimento, alla promozione commerciale e profilazione, all'utilizzo di apparecchiature di videosorveglianza e biometria
- **gestione del rapporto con amministratori, sindaci e soci:** negli adempimenti agli obblighi previsti dalla legge, da regolamenti o dalla normativa comunitaria, nonché da disposizioni impartite ad opera di Autorità a ciò preposte per legge e da Organi di Vigilanza e controllo; per finalità connesse e strumentali alla gestione del rapporto con la società o per adempiere a specifiche richieste dell'Amministratore stesso e per finalità di pubblica informazione, come ad esempio videoriprese o foto-riprese da pubblicare su riviste informative interne o anche esterne in occasione di assemblee o ad altri pubblici eventi che coinvolgano gli organi sociali

5 si tratta sia di sistemi di monitoraggio di sicurezza ICT, atte a riconoscere violazioni ai sistemi di autenticazione, alla rete, alle basi dati, alle soluzioni di sicurezza delle postazioni di lavoro e dei dispositivi mobili, sia di sistemi di monitoraggio di sicurezza fisica, destinate a individuare violazioni della protezione perimetrale, dei locali ed a trattare le violazioni segnalate dai sistemi di video-sorveglianza.

- **gestione del rapporto con i fornitori:** con riguardo sia al trattamento dei dati dei fornitori, per le finalità connesse all'apertura e all'amministrazione dl rapporto di fornitura, sia in relazione alla comunicazione agli stessi dei dati personali di cui la singola Società è titolare se previsto dal contratto di servizio

- **richieste di esercizio dei diritti degli interessati:** gli interessati possono trasmettere la propria richiesta di esercizio del diritto di accesso, rettifica, limitazione, portabilità, opposizione e cancellazione dei dati personali alle strutture del Gruppo a voce, in tal caso dovrà essere trasposta su modello standard, per iscritto consegnata a mano o tramite posta oppure in formato elettronico. In ogni caso la richiesta dovrà esser tempestivamente trasmessa all'Ufficio Privacy e Data protection, previa identificazione del mittente nel caso di consegna diretta
- **comunicazione di dati personali a terzi:** è ammessa se l'interessato vi acconsente o se ricorre uno dei casi in cui il trattamento può essere effettuato senza il consenso in quanto richiesto dalla legge, a esempio per:
  - contrasto del riciclaggio di denaro e di finanziamento del terrorismo
  - contrasto alla commercializzazione di materiale pedopornografico
  - accertamento e repressione di violazioni tributarie
  - informazioni alla Centrale rischi della Banca d'Italia e alla Centrale d'Allarme Interbancaria
  - riscontro nei confronti dell'autorità giudiziaria e, nell'ambito di una procedura esecutiva, del creditore procedente, nel rispetto delle vigenti disposizioni in materia di pignoramento presso terzi
  - riscontro a seguito di istanza di accesso alla documentazione bancaria ai sensi dell'art. 119 del Testo Unico delle leggi in materia bancaria e creditizia (TUB - d.lgs. 1 settembre 1993, n. 385)
  - comunicazione ai gestori di sistemi privati di informazione creditizie.

### 4.1 Principi applicabili al trattamento dei dati

Di seguito i principi generali nonché le possibili basi legali che possono essere utilizzate per giustificare i propri Trattamenti[6].
L'elenco dei Trattamenti svolti con le rispettive basi legali scelte dalla Società sono disponibili nel Registro dei Trattamenti ex Art. 30.

#### 4.1.1 Principio di liceità

Il Trattamento dei Dati Personali è lecito solo se si basa sul Consenso dell'Interessato o, in alternativa su un'altra base legittima prevista dal GDPR tra quelle elencate di seguito.

##### 4.1.1.1 Il consenso come base giuridica

Quanto all'espressione del Consenso vale la libertà della forma, purché sia espresso. Ne deriva che, salvo i casi in cui il GDPR richiede una manifestazione esplicita del consenso (cfr. lett. e) che segue), la Società può raccogliere un Consenso anche per comportamenti concludenti.

Il consenso è valido se è:

**a)** **Libero:** senza condizionamenti o vincoli, e per essere tale, deve essere sempre revocabile; inoltre, all'Interessato va chiarito se ha o meno l'obbligo di comunicare i propri Dati Personali e le conseguenze dell'eventuale mancata comunicazione degli stessi;

**b)** **Specifico**: deve essere richiesto un Consenso per ogni finalità perseguita dalla Società

[6] L'elencazione è supportata da esempi per far comprendere meglio alle Persone Autorizzate le possibilità di utilizzo.

**c)** **Informato**: deve essere preceduto da un'informativa privacy ex artt. 13 e 14 GDPR;
**d)** **Inequivocabile**[7]: deve esservi certezza sia rispetto al fatto che l'Interessato l'abbia prestato, che rispetto al contenuto: il Consenso non può dunque essere tacito o presunto e deve essere manifestato attraverso una dichiarazione o azione positiva inequivocabile. Nei moduli scritti la richiesta di Consenso deve essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato. La richiesta deve essere chiara, concisa, e non interferire immotivatamente con il servizio per il quale il Consenso è espresso.

**e)** **Esplicito**, solo nei seguenti casi:
i. Trattamento dei Dati Particolari ex art. 9 GDPR;
ii. Trasferimento a Paese terzo o organizzazione internazionale ex art 44 e ss. GDPR;
iii. Decisioni basate su Trattamenti Automatizzati ex art. 22 GDPR.

In questi casi il Consenso non può essere presupposto sulla base di meri fatti concludenti dell'Interessato ma va acquisito mediante un comportamento positivo e volontario dello stesso, anche se non necessariamente in forma scritta.

f) **Età dell'Interessato**: il Consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il Consenso dei genitori o di chi ne fa le veci. Qualora la Società abbia Trattato Dati Personali di un minore in assenza di tali presupposti deve applicare la limitazione del trattamento di quei dati ex art. 18 GDPR come misura cautelare a tutela del minore.

A titolo esemplificativo, salvo non siano applicabili le successive base giuridiche, nel momento il cui la Società intenda raccogliere un Consenso dagli Interessati (es. per inviare comunicazioni commerciali e/o svolgere sondaggi di customer satisfaction) deve assicurarsi di:
- fornire un'adeguata informativa privacy;
- predisporre un check-box/tick box per la raccolta del consenso, che riporti in modo chiaro per quale finalità si intende raccogliere il consenso;
- non preselezionare la scelta dell'Interessato;
- non subordinare l'erogazione di un servizio ad un consenso che per definizione è sempre facoltativo (es. non bloccare la registrazione ad un servizio se l'Interessato non ha fornito il consenso marketing).

#### 4.1.1.2 Le altre basi giuridiche

In assenza di Consenso, il Trattamento deve considerarsi lecito[8] se:

a. È necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso[9].

b. È necessario per adempiere un obbligo legale[10] al quale è soggetto il Titolare del Trattamento.

---

[7] In via esemplificativa costituisce espressione del consenso la selezione di una apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o comportamento che indichi chiaramente in tale contesto che l'Interessato accetta il Trattamento proposto.

[8] All'interno dell'interesse legittimo pare ragionevole ricomprendere anche la trasmissione di dati all'interno del Gruppo Imprenditoriale ai fini amministrativi interni, compreso il Trattamento dei Dati Personali dei dipendenti; il trattamento dati relativi al traffico in misura strettamente necessaria e proporzionata per garantire la sicurezza delle Rete Aziendale ecc. In ogni caso, occorre fare attenzione quando intende utilizzare questa base legale, valutando in anticipo se è appropriato assieme alle funzioni competenti. Per fare ciò, si eseguirà sempre una valutazione del legittimo interesse (LIA). Il risultato di tale valutazione dovrà comunque essere vagliato alla luce della normativa applicabile.

[9] A titolo esemplificativo, la Società non sarà tenuta a richiedere un Consenso per riscontrare le richieste di informazioni/dubbi dell'Interessato prevenienti da via mail; da contact form del sito Società; o per erogare un servizio che si basa su un contratto stipulato con la Società

[10] A titolo esemplificativo, la Società potrà Trattare Dati Personali dell'Interessato se previsto come obbligo dalla normativa (es. normativa fiscale; obbligo di tenuta dei Libro Unico del Lavoro; normativa antiriciclaggio ecc.).

c. È necessario per l'esecuzione di un compito svolto nel pubblico interesse[11] o per l'esercizio di pubblici poteri.

d. È necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica e solo se nessuna altra condizione di liceità può trovare applicazione[12].

e. E' un interesse legittimo del Titolare o di terzi che prevale sui diritti e sulle libertà fondamentali dell'Interessato.

#### 4.1.1.3 Le basi giuridiche aggiuntive per i Dati Particolari

Per il trattamento di Dati Particolari, ex Considerando 51 e art. 9 del GDPR, **si aggiungono** ulteriori condizioni di legittimità, per cui il Trattamento di tale categoria di dati è lecito, oltre che nelle ipotesi di cui sopra, se:

a. è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare in materia di diritto del lavoro, sicurezza sociale, protezione sociale, e se autorizzato dalla legge o dalla contrattazione collettiva nazionale in materia di lavoro[13] e in presenza di garanzie adeguate per i diritti fondamentali e gli interessi dell'Interessato

b. è necessario per tutelare un interesse vitale dell'interessato[14] o di un'altra persona in caso di incapacità fisica nel prestare il consenso

c. riguarda dati personali resi manifestamente pubblici dall'Interessato[15]

d. è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria[16]

e. è necessario per motivi di interesse pubblico rilevante sulla base del diritto nazionale o europeo[17]

f. è necessario ai fini della 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[18].

### 4.1.2 Principio di correttezza

Le Società devono trattare i Dati Personali secondo lealtà e buona fede da osservarsi in tutte le fasi del Trattamento comprese la fase preparatoria e la fase decisoria; gli interessati devono essere informati circa la raccolta, l'utilizzo e la consultazione dei loro dati e sulle ulteriori tipologie di trattamento poste in essere,

[11] Trattandosi di caso raro, questa base giuridica dovrà essere valutata internamente con le funzioni competenti prima di poter essere applicata

[12] Vedi nota 11

[13] A titolo esemplificativo, la Società potrebbe essere legittimata al Trattamento di Dati Particolari per l'esecuzione di un contratto di lavoro. In tutti questi casi, è necessario che oltre all'esecuzione di un contratto o di una richiesta contrattuale vi sia una norma o un'autorizzazione amministrativa (es. autorizzazioni generali del Garante per la protezione dei Dati).

[14] Esempio di questa base legale è il Trattamento svolto dal personale medico in fase di accreditamento ospedaliero di persona incosciente o ancora se il Trattamento è essenziale ai fini umanitari, per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione, in casi di emergenze umanitarie, di catastrofi naturali o umane etc. Tale fattispecie non appare, oggi, riferibile ad alcuna delle società del Gruppo.

[15] Esempio, il trattamento di un CV contenente Dati Particolari pubblicato dall'Interessato su un sito Internet o un social network liberamente accessibile al pubblico.

[16] Rappresenta in ogni caso un legittimo interesse della Società poter utilizzare i dati raccolti al fine di esercitare il diritto d'agire o di difendersi in giudizio.

[17] Trattandosi di caso raro, questa base giuridica dovrà essere valutata internamente con le funzioni competenti prima di poter essere applicata.

[18] Questa base giuridica è riportata a titolo di completezza ma non pare essere applicabile in via teorica ad alcuna Società.

precisando in che misura saranno effettuate al fine di garantirne la trasparenza.

### 4.1.3 Principio di trasparenza

Le informazioni e le comunicazioni relative al Trattamento dei Dati Personali che le Società devono fornire all'Interessato devono essere facilmente accessibili e comprensibili, e utilizzare un linguaggio semplice e chiaro; nel caso in cui l'Interessato effettui una richiesta di informazioni ex art. 13-14 GDPR e/o di esercizio dei diritti ex artt. 15-22 GDPR (diritto di accesso, rettifica, cancellazione/oblio, portabilità, limitazione del trattamento) il riscontro, in virtù del principio in oggetto, deve essere dato, senza ritardo, al più tardi entro un mese, prorogabile fino a tre mesi con adeguata motivazione.

### 4.1.4 Principio di limitazione delle finalità

I Dati personali devono essere trattati per finalità determinate, esplicite e legittime, ossia per finalità lecite e comunicate chiaramente all'Interessato affinché sia in grado di conoscere le specifiche finalità, chiare ed univoche del Trattamento dei suoi dati.

Un trattamento di Dati Personali successivo e diverso rispetto alle finalità iniziali può essere compatibile sulla base di una congrua valutazione ad opera delle Società basata su:

- 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.

È tuttavia riconosciuto *ex lege* compatibile l'ulteriore Trattamento per finalità di archiviazione nel pubblico interesse, per finalità statistiche, di ricerca scientifica e storica ovvero basato sul diritto nazionale o europeo e che costituisce una misura necessaria e proporzionata in una società democratica per salvaguardare, in particolare, importanti obiettivi di interesse pubblico generale.

Qualora non si rientri nei casi precedenti, la Società ha l'obbligo di informare l'Interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi al Trattamento ex art. 18 GDPR.

### 4.1.5 Principio di minimizzazione dei dati

I Dati Personali Trattati devono essere pertinenti, adeguati e limitati rispetto alle finalità - cd. "minimizzazione dei dati"; deve essere minimizzata la quantità dei dati raccolti quanto più possibile, e limitata ai dati strettamente necessari alle finalità predeterminate.

La minimizzazione si estende anche alla configurazione dei software e dei sistemi informativi, sin dalla fase della loro progettazione, utilizzati per trattare i Dati Personali in modo da ridurre al minimo il loro uso (cd. data protection by design); nonché allo sviluppo di tecnologie e/o processi con l'obiettivo di raccogliere ed elaborare solo i dati personali strettamente necessari per consentire all'interessato di fruire delle funzionalità richieste assicurando by default un trattamento legittimo (cd. data protection by default).

### 4.1.6 Principio di esattezza

Le Società devono assicurare l'accuratezza e la qualità dei Dati Personali, soprattutto quando il dato viene raccolto presso terzi, trattando dati esatti e aggiornati. In applicazione del principio in oggetto, l'Interessato ha un diritto di rettifica e laddove i suoi dati siano inesatti o non aggiornati, ha il diritto di ottenere, in via cautelativa, la limitazione del Trattamento per tutto il periodo necessario alla Società per le opportune verifiche e per effettuare, ove necessario, le procedure di rettifica. Infine, se non è concretamente possibile effettuare l'aggiornamento o la rettifica dei dati, l'Interessato ha il diritto di ottenere la cancellazione degli stessi. Il fatto che i dati siano esatti e aggiornati non rappresenta solo un diritto dell'Interessato, ma specularmente, un vero e proprio dovere per le Società, che devono rendere note le eventuali rettifiche operate sui dati all'Interessato.

#### 4.1.7 Principio di limitazione della conservazione

Di regola i dati devono essere conservati in una forma che permetta l'identificazione degli Interessati per un lasso di tempo non superiore al conseguimento delle finalità del Trattamento, onde evitare un abuso contrario ai principi di correttezza, trasparenza e liceità.

#### 4.1.8 Principio di integrità e riservatezza

Ai dati deve essere garantita un'adeguata sicurezza; le informazioni devono essere salvaguardate nella loro esattezza (integrità) e difese da intrusioni e alterazioni non autorizzate (riservatezza). Le Società devono adottare misure tecniche e organizzative affinché siano impediti l'accesso e l'utilizzo non autorizzato ai Dati Personali e alle attrezzature impiegate per il Trattamento.

#### 4.1.9 Principio di responsabilizzazione

Si sostanzia nel rispetto dei principi suddetti e nella capacità della Società di comprovarlo. Attraverso questa policy e i documenti di rango inferiore tempo per tempo redatti, che costituiscono il **Modello Organizzativo Privacy**, le Società danno evidenza di aver messo in atto misure adeguate ed efficaci per dimostrare, su richiesta dell'Autorità di Controllo, la conformità delle attività di Trattamento al GDPR, compresa l'efficacia delle misure stesse.

### 4.2 Criteri sulla conservazione dei dati personali

Con l'entrata in vigore del GDPR, le Società hanno l'obbligo di definire il periodo di conservazione dei Dati Personali oppure, se ciò non è possibile, i criteri utilizzati per determinare tale periodo.

In considerazione del fatto che determinare un criterio astratto è più semplice, oltre che metodologicamente più corretto, per arrivare ad uno specifico periodo di conservazione, la Società elencherà in un documento di rango inferiore i macro-criteri di conservazione identificati.

Progressivamente, si procederà, secondo il principio di responsabilizzazione, a definire, ove possibile, i periodi esatti di conservazione.

I criteri e i periodi di conservazione sono costantemente aggiornati nel Registro dei Trattamenti ex art. 30, se previsto, e in ogni caso nelle fonti previste.

#### 4.1.10 Criterio di necessità

Vengono conservati tutti i Dati Personali necessari a raggiungere lo scopo per il quale sono stati raccolti e per il tempo necessario a raggiungere tale scopo (es.: dati conservati in costanza di rapporto contrattuale e per tutta la sua durata).

#### 4.1.11 *O*bbligo di Legge

Vengono conservati tutti i Dati Personali che la normativa vigente (es.: fiscale, giuslavoristica) impone di conservare, per il tempo richiesto dalla normativa stessa.

#### 4.1.12 Opportunità

Vengono conservati i Dati Personali che la legge dà facoltà di conservare, per il tempo suggerito dalla normativa oppure stabilito dal Titolare.

È il caso ad esempio dei dati conservati per finalità di difesa in giudizio da azioni di natura contrattuale o extracontrattuale. Nel primo caso, verranno conservati solo – ed esclusivamente - i Dati Personali necessari, ad esempio, ad avere correttamente erogato il servizio contrattualizzato, per dieci anni dalla cessazione del rapporto contrattuale; nel secondo caso, si conserveranno per cinque anni i dati necessari a difendersi in giudizio da azioni di natura extracontrattuale. Ancora, è il caso dei dati raccolti e trattati per finalità di marketing, riferiti a soggetti con cui non si ha più un rapporto contrattuale, conservati fino alla revoca del Consenso da parte dell'Interessato.

### 4.3 Utilizzo degli Strumenti Aziendali

Specifica regolamentazione dei gruppo dovrà regolamentare l'utilizzo degli Strumenti Aziendali della società nonché degli eventuali Strumenti Personali autorizzati per uso lavorativo.
La stessa dovrà seguire le prescrizioni:

- delle linee guida sull'uso della posta elettronica ed internet emanate con la delibera n. 13 del 1 marzo 2007 (doc. web n. 1387522) del Garante per la protezione dei dati e successivi provvedimenti tra cui il provvedimento *Accesso alla posta elettronica dei dipendenti* del 22 dicembre 2016;
- dei Garanti Europei ("Gruppo di Lavoro Articolo 29") indicate nell'Opinione 2/2017;
- del documento "eCommunication guidelines" del Garante Europeo per la Privacy (EDPS).

# 5 Definizione del rischio

Il Rischio di non conformità alla normativa in materia di protezione dei dati personali è il rischio di incorrere in sanzioni amministrative, illeciti penali o danni reputazionali per l'inosservanza degli obblighi previsti per il trattamento dei dati personali.

Qualunque persona fisica o giuridica tratti dati personali è tenuta all'osservanza delle disposizioni e degli obblighi stabiliti dalla normativa e può essere oggetto sia di azioni risarcitorie che di accertamenti e provvedimenti delle Autorità di Controllo e/o dell'Autorità Giudiziaria.

Il GDPR protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, disciplinando le diverse operazioni di gestione dei dati («trattamento»).

Per le **persone giuridiche** la normativa riconosce la sola facoltà di opporsi all'invio di materiale pubblicitario, alla vendita diretta o al compimento di ricerche di mercato o di promozione commerciale attraverso sistemi di comunicazione elettronica.

Obiettivo della normativa è "la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale" intendendo tale protezione come "un diritto fondamentale". "L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano."[19]

A tutela degli interessati il GDPR prevede che tutti coloro aventi responsabilità nel trattamento di dati personali adottino specifiche e adeguate misure di sicurezza; esse riguardano il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali che configurano i livelli di protezione necessari a ridurre al minimo i rischi di distruzione, perdita o indisponibilità, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta

# 6 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 secondo il quale ciascun rischio viene assunto a livello decentrato ma sotto il coordinamento e l'indirizzo della Capogruppo mentre le attività di gestione del rischio vengono svolte in via accentrata dalla Capogruppo.

[19] Riferimento: GDPR - Considerando 1

La 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.

Alla Capogruppo sono assegnate le seguenti responsabilità:

• assicurare un'adeguata attuazione del modello di governo del rischio di non conformità sia a livello di singola società del Gruppo che a livello consolidato;

• assicurare che il modello di governo del rischio di non conformità sia predisposto nel rispetto di quanto definito dalle Autorità di Vigilanza, tenendo conto delle specificità del Gruppo e delle singole società del Gruppo che lo compongono.

L'attuazione di tali principi avviene attraverso l'adozione del modello di governo del rischio di non conformità alla normativa in materia di protezione dei dati personali formalizzato nella presente Policy che garantisce:

- chiarezza nell'attribuzione dei ruoli e delle responsabilità;
- separazione tra le funzioni preposte ai processi di assunzione e gestione operativa del rischio da quelli preposti alla gestione e controllo del rischio di non conformità garantendo l'indipendenza dei ruoli e delle responsabilità.

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.

Per assicurare la conformità alle disposizioni in materia di trattamento dei dati personali, la Capogruppo ha definito per il Gruppo BPER un sistema di misure organizzative e procedure operative per la gestione degli adempimenti in materia di privacy che rispetti i principi di privacy by design e privacy by default richiesti dal Regolamento e garantisca l'esercizio dei diritti dell'interessato

Le Società del Gruppo BPER rivestono il ruolo di "Titolare del trattamento dei dati personali" delle categorie di interessati (clienti, dipendenti, collaboratori esterni, amministratori, sindaci, fornitori, ecc.) dei quali trattino, anche occasionalmente, dati personali e pertanto sono tenute all'osservanza degli obblighi previsti.

Le Società del Gruppo possono rivestire anche il ruolo di "Responsabili del Trattamento dei dati personali", nell'ambito del quale sono altrettanto tenute all'osservanza di specifici obblighi.

I rispettivi Consigli di Amministrazione hanno la responsabilità di definire, secondo gli indirizzi forniti dalla Capogruppo:

- finalità e modalità dei trattamenti di dati personali effettuati nel proprio ambito
- efficace articolazione dei presidi e delle responsabilità a livello organizzativo
- strumenti impiegati e misure di sicurezza adeguate.

Poiché il Sistema informativo del Gruppo BPER prevede in linea generale che:

- le Società del Gruppo esternalizzino le risorse ed i servizi ICT, la funzione di sicurezza informatica e del sistema di gestione dei dati ("full outsourcing del Sistema informativo del Gruppo")
- le funzioni del Sistema informativo delle Banche italiane del Gruppo siano accentrate presso una società strumentale di natura informatica del Gruppo, a cui è consentita la sub-esternalizzazione extra-gruppo di servizi ICT
- l'Amministratore Delegato della Capogruppo abbia la responsabilità di assicurare la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema informativo di Gruppo e conferisca al Chief Operating Officer – C.O.O. di Gruppo i poteri per la realizzazione e gestione del sistema informativo di Gruppo
- il Chief Information Officer di Gruppo, che riporta al C.O.O., sia responsabile della funzione di direzione strategica del sistema informativo di Gruppo

la Capogruppo ha individuato per il Gruppo misure organizzative e di sicurezza specifiche per il trattamento e la protezione dei dati personali attraverso strumenti elettronici che permettono un efficace e dettagliato presidio anche sui singoli elementi di informazione presenti nei diversi database utilizzati.

Le misure di sicurezza predisposte riguardano i seguenti servizi:

- erogazione del sistema informativo e delle relative applicazioni

- fornitura e conservazione di idonei supporti di memorizzazione dei dati
- fornitura del servizio di Disaster Recovery
- custodia e controllo periodico dei dati relativi ai file sequenziali di registrazione (log) di accesso ai sistemi informatici di cui Bper Services ha il controllo e contenenti dati personali di tutte le Banche e Società consorziate, ai sensi di quanto disposto dal provvedimento del Garante della Privacy del 27/11/08 relativo agli Amministratori di Sistema.

Per quanto riguarda la gestione degli accessi al Sistema informativo aziendale sono state definite misure e accorgimenti per garantire la sicurezza, da utilizzi fraudolenti e da aggressioni esterne, dei dati e delle informazioni trattate.

Relativamente alle società non allineate al sistema informativo, le misure per garantire la sicurezza, da utilizzi fraudolenti e da aggressioni esterne, dei dati e delle informazioni trattate attraverso il sistema informativo sono assicurate secondo quanto stabilito nelle Linee Guida di Gruppo del Sistema Informativo.

# 7 Propensione al rischio

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

Il Gruppo considera pertanto necessario che l'operatività sia improntata al rispetto formale e sostanziale delle norme vigenti. Tale indicazione è posta in particolare con riferimento alle attività di business, per le quali dovrà essere perseguita la piena conformità alle normative che regolamentano l'operatività svolta.

**Unità organizzative della Capogruppo**

**Compiti di Indirizzo e coordinamento**

*Responsabile della Protezione Dati (DPO)*: figura unica per tutte le società italiane[20] appartenenti al gruppo bancario, cui sono affidati i compiti previsti dall'art. 39 del GDPR. In sintesi, il DPO fornisce al titolare/Responsabile del trattamento il supporto indispensabile ad assicurare l'osservanza del Regolamento.

**Compiti per BPER**

*Delegato Privacy Aziendale:* figura a cui il Titolare del trattamento dei dati (Consiglio di Amministrazione) delega funzioni e compiti propri.

Il Delegato esercita le sue 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.

*Ufficio Privacy e Data protection:* unità organizzativa con competenze specialistiche in materia, che ha il compito di supportare il DPO, il Delegato, Privacy Expert aziendali e le altre strutture di BPER nei relativi adempimenti. L'Ufficio svolge anche il ruolo di "presidio specialistico"[21] di Compliance per gli ambiti normativi definiti tempo per tempo nella regolamentazione della funzione Compliance del Gruppo.

[20] BPER International SA Lussemburgo si doterà di un proprio DPO, individuato secondo i medesimi criteri e le medesime logiche definite dalla Capogruppo, che ricoprirà anche il ruolo di *Privacy Contact Aziendale* nei confronti del DPO del Gruppo.

[21] In particolare, identifica e valuta il rischio di non conformità nella prospettiva di Gruppo e rispetto alle singole Società, valutando l'adeguatezza dei presidi per la sua prevenzione/mitigazione e proponendo gli interventi ritenuti necessari per assicurare il maggior livello di conformità ed adeguatezza. Presta consulenza ed assistenza nei confronti degli Organi aziendali e delle Unità Organizzative del Gruppo nell'applicazione e nell'interpretazione delle norme.

*Direzione Risorse Umane:* garantisce nel corso delle assunzioni e dei trasferimenti dei dipendenti, la corretta esecuzione degli adempimenti privacy relativi alle istruzioni, alla formazione per gli incaricati ed alla conduzione del rapporto di lavoro, definiti dal Titolare del trattamento.

*Ufficio Architetture e sicurezza:* garantisce la corretta applicazione dei criteri in materia di definizione e monitoraggio dei profili abilitativi al sistema informativo secondo principi di minimo privilegio e separazione dei compiti e secondo gli indirizzi del Titolare del trattamento; sentito il parere della Funzione Compliance, sottopone all'approvazione del Consiglio di Amministrazione di Capogruppo i criteri per l'individuazione degli AdS nelle società del Gruppo, assicura il corretto adempimento delle disposizioni del Titolare in materia di videosorveglianza e biometria.

*Responsabile del Sistema di Whistleblowing:* assicura il corretto adempimento degli obblighi in ambito privacy relativi al Sistema e definiti dal Titolare del trattamento, oltre alla identificazione degli Incaricati al trattamento dei dati del Sistema.

*Direzione Commerciale:* assicura la corretta applicazione degli indirizzi del Titolare in materia di

- trattamento dei dati della clientela al momento dell'instaurazione del rapporto;
- registrazione delle telefonate dei clienti per gli ordini di acquisto e vendita titoli;

Assicura inoltre il corretto adempimento degli obblighi in ambito privacy relativi alla promozione commerciale, definiti dal Titolare del trattamento

*Area Crediti:* assicura la corretta applicazione degli indirizzi del Titolare in materia di consultazione dei SIC e preavviso di segnalazione relativamente ai dati della clientela

*Direzione Affari Generali:* assicura la corretta applicazione degli indirizzi del Titolare nell'istruire i riscontri relativi ai reclami; assicura il corretto adempimento degli obblighi in ambito privacy relativi al trattamento dei dati degli Amministratori, dei Sindaci e dei Soci.

*Servizio Acquisti:* assicura la corretta applicazione degli indirizzi del Titolare in materia di trattamento dei dati personali dei fornitori e provvede alla Nomina a responsabile quando necessario utilizzando il modello di Privacy agreement predisposto per tutto il Gruppo.

**Compiti per altre Società del Gruppo**

*Ufficio Privacy e Data protection:* unità organizzativa istituita presso la Capogruppo con competenze specialistiche in materia, che ha il compito di supportare Delegati, Privacy Expert aziendali e le altre strutture delle Società del Gruppo nei relativi adempimenti, sulla base di un contratto di prestazione di servizi. L'Ufficio svolge anche il ruolo di "presidio specialistico"[22] di Compliance per gli ambiti normativi definiti tempo per tempo nella regolamentazione della funzione Compliance del Gruppo.

*Responsabile del Sistema di Whistleblowing:* esercita la propria funzione in base ad un contratto di esternalizzazione in qualità di *outsourcer*, esegue le attività già previste per BPER.

**Unità organizzative della Società**

**Compiti per la Società**

*Delegato Privacy Aziendale:* figura a cui il Titolare del trattamento dei dati (Consiglio di Amministrazione della *Legal Entity*) delega funzioni e compiti propri. Questi è individuato, di norma, nel Direttore generale/Amministratore delegato della Società.

Il Delegato esercita le sue funzioni tramite i poteri decisionali, organizzativi e di disposizione, sia ordinari

[22] In particolare, identifica e valuta il rischio di non conformità nella prospettiva di Gruppo e rispetto alle singole Società, valutando l'adeguatezza dei presidi per la sua prevenzione/mitigazione e proponendo gli interventi ritenuti necessari per assicurare il maggior livello di conformità ed adeguatezza. Presta consulenza ed assistenza nei confronti degli Organi aziendali e delle Unità Organizzative del Gruppo nell'applicazione e nell'interpretazione delle norme.

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.

*Privacy Contact Aziendale*[23]: figura prevista in ciascuna Società italiana del Gruppo, incaricata di svolgere compiti di raccordo informativo e rappresentanza del DPO del Gruppo, col quale opera a stretto contatto.

*Privacy Specialist Aziendale*[24]: figura prevista in ciascuna Banca italiana del Gruppo, incaricata di svolgere compiti operativi e di raccordo informativo, che opera in stretto contatto con l'Ufficio Privacy e Data protection della Capogruppo.

**Organi Societari della Capogruppo**

**Ruoli e responsabilità di Indirizzo e coordinamento**

Il *Consiglio di Amministrazione*, in qualità di Organo con Funzione di Supervisione Strategica, nell'ambito della generale responsabilità di governo del rischio stabilisce, tra l'altro, univoci indirizzi e adempimenti affinché le relazioni d'affari siano improntate alla sana e prudente gestione nonché a criteri di buona fede e correttezza.

Nel ruolo di indirizzo e coordinamento esercitato nei confronti delle Società del Gruppo:

- approva la "Policy di Gruppo per il Governo del rischio di non conformità – Protezione dei dati personali" in cui sono definiti:
    - indirizzi e regole uniformi per le Società del Gruppo per il rispetto della conformità alla normativa in parola
    - un sistema di "presidi per la prevenzione del rischio di non conformità alla normativa in materia di privacy" articolato in base alla dimensione e complessità delle strutture e dei modelli delle Società del Gruppo
- su proposta del Responsabile della Funzione Sicurezza Logica di Capogruppo, stabilisce criteri validi per il Gruppo relativamente alla definizione e monitoraggio dei profili abilitativi degli incaricati secondo principi di minimo privilegio e separazione dei compiti
- definisce principi validi per il Gruppo relativamente alle disposizioni normative sul trattamento di dati personali effettuato dagli Amministratori di Sistema
- approva, su proposta del *Chief Operating Officer*, i criteri che le Società del Gruppo adottano per assicurare la conformità alle previsioni normative sul trattamento dei dati personali dei dipendenti acquisiti accedendo alla loro posta elettronica e ai loro accessi alla rete internet effettuati durante la prestazione di lavoro
- approva, su proposta del Delegato Privacy, i criteri validi per il Gruppo in merito all'individuazione e la gestione delle operazioni bancarie sospette di violazione ai sensi della normativa sul trattamento di dati personali della clientela effettuato dai dipendenti delle banche e delle società facenti parte di

[23] Compiti e responsabilità risultano compatibili con il ruolo di Referente di funzione aziendale di controllo di 2° livello

[24] Soggetto o unità organizzativa individuata presso ciascuna banca del gruppo, in virtù della tipologia e della natura dei trattamenti svolti, che pur prestando anche altre attività funge da entry point / contatto verso la capogruppo.

gruppi bancari

**Ruoli e responsabilità esercitati per Bper**

Il *Consiglio di Amministrazione* assicura la corretta applicazione a livello aziendale degli indirizzi e regole definiti per il Gruppo e e la realizzazione del modello di presidi per la prevenzione del rischio di non conformità in materia di Privacy; nomina il Delegato Privacy aziendale cui delega funzioni e compiti propri, mantenendo tuttavia in carico al Consiglio stesso le responsabilità amministrative, le azioni risarcitorie, gli accertamenti e i provvedimenti del Garante Privacy e le responsabilità civili e penali non riconducibili al Delegato

**Organi Societari della Società**

I *Consigli di Amministrazione* di ciascuna Banca o Società del Gruppo, secondo gli indirizzi forniti dalla Capogruppo e recepiti attraverso l'approvazione della "Policy di Gruppo per il Governo del rischio di non conformità – Protezione dei dati personali", hanno la responsabilità di definire:

- finalità e modalità dei trattamenti di dati personali effettuati nel proprio ambito
- adeguata ed efficace articolazione dei presidi e delle responsabilità a livello organizzativo
- strumenti impiegati e misure di sicurezza.

## 8 Limiti di esposizione e operativi

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

## 9 Assunzione e mitigazione

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

## 10 Gestione del rischio

Per assicurare il rispetto degli obblighi previsti per le Società del Gruppo che trattano dati personali, il Consiglio di Amministrazione della Capogruppo ha definito per il Gruppo un Sistema di "presidi per la prevenzione del rischio di non conformità alla normativa in materia di privacy", attraverso procedure e processi organizzativi, articolato in base alla dimensione e complessità delle strutture e dei modelli delle Società del Gruppo.

In linea generale il sistema dei presidi è progettato per tenere conto delle peculiarità del business esercitato da ciascuna società del Gruppo:

- Il Titolare del trattamento dei dati di ciascuna Società è tenuto a impartire istruzioni su come dipendenti e personale assimilabile ("autorizzati") devono trattare i dati personali nell'ambito dell'attività lavorativa

- L'accesso al sistema informativo delle Società del Gruppo deve essere gestito nel rispetto di quanto stabilito in merito dalla normativa *privacy*, secondo principi di pertinenza e non eccedenza, allo scopo di prevenire la possibilità di illeciti trattamenti di dati personali
- I Responsabili delle unità organizzative hanno il compito di garantire il rispetto degli adempimenti privacy nelle istruzioni alle persone autorizzare da lui coordinati.
- I Responsabili delle unità organizzative presso cui vengono svolte azioni di promozione commerciale assicurano che gli addetti svolgano tali attività nel rispetto delle indicazioni impartite dalla azienda.
- I Responsabili delle Unità Organizzative presso cui sono installati sistemi di videosorveglianza e / o di rilevazione biometrica delle impronte digitali assicurano che gli addetti svolgano le attività di gestione nel rispetto delle indicazioni impartite dalla azienda.
- La comunicazione a terzi di dati personali relativi ad un soggetto è ammessa, di norma, se lo stesso vi acconsente o se ricorre uno dei casi in cui il trattamento può essere effettuato senza il consenso.

**Unità organizzative della Capogruppo**

**Compiti di Indirizzo e coordinamento**

**Compiti per Bper**

*Ufficio Privacy e Data protection* per BPER Banca e per le diverse *legal entity* per cui presta tale servizio:

- supporta il Delegato Privacy Aziendale nell'esercizio delle responsabilità affidate
- supporta le funzioni aziendali nell'esercizio delle responsabilità affidate redige e aggiorna i modelli di "istruzione per gli autorizzati" destinate ai dipendenti e al personale assimilabile
- redige e aggiorna i modelli di "Contratto per il Trattamento dei Dati Personali", siano essi riferiti a rapporti infragruppo o extragruppo (c.d. Responsabili del trattamento dei dati personali per conto dei Titolari), identificando le singole fattispecie da utilizzare sulla base della natura e della tipologia del contratto/accordo/trattamento redige ed aggiorna i modelli di "Informative privacy" destinate ai dipendenti e al personale assimilabile, alla clientela per BPER e per le diverse *legal entity* per cui presta tale servizio, agli Amministratori e ai Sindaci
- supporta il DPO nella tenuta del Registro delle attività di trattamento: nel caso che sia necessario un aggiornamento del Registro delle attività di trattamento, effettua un'analisi complessiva del trattamento, coinvolgendo le U.O responsabili dell'attività e sottopone gli esiti alla valutazione del DPO
- nei casi previsti dall'art. 35 del GDPR qualora sia necessario procedere con una Privacy Impact Assessment PIA, con il supporto del Process Owner provvede alla ricognizione del contesto oggetto di valutazione ed esamina il trattamento, le sue finalità, la necessità e la proporzionalità di questo rispetto alle finalità, valuta i rischi potenziali nei possibili impatti per i diritti e le libertà degli interessati coinvolti dal trattamento e individua le misure di mitigazione. Coinvolge il DPO per un parere in merito alla valutazione d'impatto sulla protezione dei dati e sullo svolgimento della stessa come previsto dall'art. 39 del GDPR
- esegue le analisi relative alla presenza di trattamenti basati sul legittimo interesse, come previsto dall'art. 6 comma 1 lettera *f)* del GDPR, documentando il processo di valutazione condotto. Coinvolge il DPO per un parere in merito a tale valutazione sul bilanciamento di interesse rispetto diritti e libertà degli interessati, oltre che sullo svolgimento della stessa
- valuta le segnalazioni ricevute di potenziali *data breach* e verifica se si sia manifestata una violazione dei dati personali, informa contestualmente il DPO allo scopo di determinare congiuntamente il perimetro ed i volumi della violazione e nel caso procedere alle comunicazioni di cui agli articoli 33 e34 del Regolamento
- riscontra le richieste di accesso, rettifica, limitazione, portabilità, opposizione e cancellazione degli interessati senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa.

- gestisce l'analisi preliminare degli *alert* (prodotti da applicativi informatici predisposti sulla base dei criteri di estrazione) come previsto dal modello adottato per assicurare il rispetto dei princìpi in materia di Circolazione delle informazioni e tracciamento delle operazioni bancarie di dati personali della clientela[25] effettuato dai dipendenti delle banche e delle società anche diverse dalle banche ma parte di gruppi bancari. Qualora l'evento non sia giustificabile dal Responsabile, l'*alert* verrà analizzato dalla funzione Revisione Interna di Gruppo e comunicato alla funzione Risorse Umane di Gruppo per la dovuta informativa al dipendente. Sulla base dei dati statistici prodotti dal processo, propone l'aggiornamento dei criteri di estrazione per efficientare il presidio.

*Direzione Risorse Umane*

- garantisce la corretta esecuzione degli adempimenti privacy nel corso delle assunzioni e dei trasferimenti delle risorse, relativamente a istruzioni e formazione per gli incaricati
- esegue quanto disposto dalla normativa in materia di protezione dei dati personali dei dipendenti, trattati per adempiere ad obblighi previsti dalla legge e/o derivanti dal contratto di lavoro
- si adopera per il corretto adempimento degli obblighi in ambito privacy relativi all'instaurazione e conduzione del rapporto di lavoro con i dipendenti
- assicura il rispetto delle misure definite dall'autorità di controllo che i datori di lavoro devono adottare nel trattamento dei dati personali dei dipendenti acquisiti accedendo alla loro posta elettronica e ai loro accessi alla rete internet impiegati durante la prestazione di lavoro.

*Architettura e Sicurezza*

- assicura che venga adempiuto quanto disposto dalla normativa, anche in materia di misure di protezione dei dati personali e la definizione e monitoraggio dei profili abilitativi degli incaricati secondo principi di minimo privilegio e separazione dei compiti.
- sentito il parere del Data Protection Officer, sottopone all'approvazione del Consiglio di Amministrazione di BPER i criteri per l'individuazione degli AdS nelle società del Gruppo26. Il controllo dei log è demandato ad ogni responsabile dell'unità organizzativa che annovera AdS nel proprio organico.
- nell'ambito delle attività di valutazione di un incidente informatico qualora ravvisi un potenziale coinvolgimento dei dati personali degli interessati informa tempestivamente il DPO e l'Ufficio Privacy e Data protection

*Responsabile del Sistema di Whistleblowing*

- assicura la corretta esecuzione degli adempimenti privacy relativi alle istruzioni per gli incaricati, definiti dal Titolare del trattamento (e, nel caso sia istituito, dal Delegato) e che venga adempiuto quanto disposto dalla normativa, anche in materia di misure di sicurezza previste per il correlato trattamento dei dati personali.

*Direzione Commerciale*

- assicura la corretta applicazione degli adempimenti in materia di trattamento dei dati della clientela al momento dell'instaurazione del rapporto mediante la consegna dell'informativa e la raccolta dei consensi/dinieghi
- assicura la corretta applicazione degli indirizzi della Capogruppo in materia di registrazione delle telefonate per gli ordini di acquisto e vendita titoli, anche in merito alle misure di sicurezza previste per il correlato trattamento dei dati personali

*Direzione Affari Generali*

- assicura la correttezza del trattamento dei dati personali degli Amministratori e Sindaci e provvede alla consegna della relativa Informativa privacy dedicata e alla raccolta documentata dei consensi e dei dinieghi relativi al trattamento dei dati personali, come previsto dalla normativa.

  istruisce i reclami pervenuti in ambito Privacy e i ricorsi all'Autorità di controllo e fornisce riscontro

[25] Provvedimento n.192 del 12.05.2011 recante "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie".

[26] Provvedimento Garante Privacy 27 novembre 2008 – "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema".

nei termini normativi avvalendosi se necessario del supporto dell'Ufficio Privacy e Data protection

*Servizio Acquisti*

- provvede nei confronti del fornitore alla nomina a Responsabile ove ne ricorrano i presupposti sulla base delle determinazioni per l'ambito privacy disciplinate nei singoli contratti, utilizzando i template di Privacy agreement ricevuti dall'Ufficio Privacy e Data protection, sottoponendo all'attenzione di quest'ultimo eventuali casi particolari
- predispone apposito documento a disposizione della clientela in cui sono elencate le società esterne e tutti i soggetti terzi cui ogni legal entity comunica o trasmette dati personali con ruolo di "Titolari del trattamento", oppure nominati Responsabili

**Compiti per altre Società del Gruppo**

*Ufficio Privacy e Data protection* svolge i medesimi compiti di cui è incaricato per BPER per le legal entities che hanno sottoscritto un accordo di esternalizzazione con la Capogruppo, sulla base di quanto riportato nell'accordo stesso.

*Architettura e Sicurezz*a svolge i medesimi compiti di cui è incaricato per BPER per le legal entities che hanno sottoscritto un accordo di esternalizzazione con la Capogruppo, sulla base di quanto riportato nell'accordo stesso.

*Responsabile del Sistema di Whistleblowing* svolge i medesimi compiti di cui è incaricato per BPER

*Servizio Acquisti* svolge i medesimi compiti di cui è incaricato per BPER per le legal entities che hanno sottoscritto un accordo di esternalizzazione con la Capogruppo, sulla base di quanto riportato nell'accordo stesso.

**Unità organizzative della Società**

Il Titolare del trattamento dei dati di ciascuna Società è tenuto a impartire istruzioni su come dipendenti e personale assimilabile ("autorizzati") devono trattare i dati personali nell'ambito dell'attività lavorativa.

I Responsabili delle unità organizzative hanno il compito di garantire il rispetto degli adempimenti privacy nelle istruzioni alle persone autorizzare da lui coordinati.

**Compiti per la Società**

La funzione Risorse Umane di ciascuna società assicura gli stessi adempimenti previsti per l'omologa funzione di BPER

La funzione Sicurezza Logica di ciascuna Società ha la responsabilità di individuare e controllare l'operato degli AdS di ciascuna Società sulla base dei criteri indicati dalla Capogruppo. Assicura gli stessi adempimenti previsti per l'omologa funzione di BPER

La funzione Commerciale di ciascuna società assicura gli stessi adempimenti previsti per l'omologa funzione di BPER

La funzione Affari Generali di ciascuna società assicura gli stessi adempimenti previsti per l'omologa funzione di BPER

La funzione Acquisti di ciascuna società assicura gli stessi adempimenti previsti per l'omologa funzione di BPER

**Compiti per altre Società del Gruppo**

Non previsti

**Organi Societari della Capogruppo**

**Ruoli e responsabilità di Indirizzo e coordinamento**

Il Consiglio di Amministrazione della Capogruppo ha adottato un modello organizzativo di Gruppo per la corretta esecuzione degli adempimenti privacy relativi alle istruzioni e alla formazione degli autorizzati, e al trattamento dei dati personali

Il Consiglio di Amministrazione della Capogruppo

- assicura l'adempimento di quanto disposto dalla normativa in materia di misure di protezione dei dati personali
- assegna al Responsabile della Direzione Risorse Umane il compito di assicurare la corretta esecuzione degli adempimenti privacy relativi alle istruzioni e alla formazione, per gli incaricati, nell'instaurazione e conduzione del rapporto di lavoro, anche riguardo al rispetto della disciplina in materia di controllo a distanza dei lavoratori
- stabilisce criteri validi per il Gruppo che prevedono profili abilitativi degli incaricati secondo principi di minimo privilegio e separazione dei compiti e criteri con cui individuare gli AdS, il controllo ed archiviazione dei log prodotti dagli AdS
- assicura il rispetto della disciplina in materia di "Sistemi interni di segnalazione delle violazioni"27 mediante l'adozione di un sistema interno di segnalazione detto "Sistema di Whistleblowing" accentrato che consente ai dipendenti di segnalare, in modo diretto e con garanzia di riservatezza, eventuali comportamenti illegittimi
- assicura che siano comunicati al cliente al momento dell'instaurazione del rapporto:
  - i trattamenti a cui sono sottoposti i suoi dati personali
  - le modalità con cui potrà esercitare i suoi diritti relativamente ai propri dati personali
  - a quali altri Titolari e Responsabili esterni la Società vengono comunicati tali dati
- ogni attività a carattere promozionale e commerciale venga svolta nel rispetto delle prescrizioni dell'Autorità e previa verifica che la clientela destinataria abbia previamente fornito il dovuto consenso.
- ha definito un modello organizzativo di Gruppo relativo al trattamento dei dati personali degli Amministratori e Sindaci che prevede la consegna dell'Informativa privacy dedicata e la raccolta documentata dei consensi e dei dinieghi relativi al trattamento dei dati personali
- ha definito un modello organizzativo di Gruppo per i rapporti con i fornitori e che prevede, nei casi previsti dalla normativa, il ricorso ad accordi scritti ad hoc in sede di instaurazione della relazione.

**Ruoli e responsabilità esercitati per Bper**

Il Consiglio di Amministrazione assume le medesime responsabilità per BPER e per il Gruppo

**Organi Societari della Società**

I Consigli di Amministrazione delle Società secondo gli indirizzi impartiti dalla Capogruppo esercitano le medesime attribuzioni del Consiglio di amministrazione della Capogruppo.

[27] D.Lgs. del 12 maggio 2015, n. 72 – Attuazione della Direttiva 2013/36/UE (CRD IV) relativa ai "Sistemi interni di segnalazione delle violazioni".

## 11 Flussi informativi

Tale paragrafo non è valorizzato in quanto non sono previsti **flussi informativi "standard"** nell'ambito della Policy in esame.

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".