IBL Banca
GRUPPO BANCARIO

POLICY DI GRUPPO IN MATERIA DI DATA PROTECTION

A. MODALITA' DI GESTIONE DEL DOCUMENTO 3

B. PREMESSA 4

1. SCOPO DEL DOCUMENTO 4
2. APPLICABILITÀ 4
3. RIFERIMENTI 4
3.1. RIFERIMENTI ESTERNI 5
3.2. RIFERIMENTI INTERNI 6
4. AGGIORNAMENTI 6
5. GLOSSARIO 6
6. LIVELLO GERARCHICO 10

C. PARTE PRIMA - MODELLO ORGANIZZATIVO DATA PROTECTION ... 11

1. RUOLI E RESPONSABILITÀ 11
1.1 TITOLARE DEL TRATTAMENTO 14
1.2 COMITATO DATA PROTECTION 15
1.3 DATA PROTECTION OFFICER 16
1.4 RESPONSABILE INTERNO DEL TRATTAMENTO 17
1.5 RESPONSABILE ESTERNO DEL TRATTAMENTO 18
1.6 ADDETTI AL TRATTAMENTO 19
1.6.1. Assunzione e formazione del personale 19
1.7 AMMINISTRATORI DI SISTEMA 20

D. PARTE SECONDA - I PRINCIPALI ADEMPIMENTI DATA PROTECTION 21

1. GESTIONE DEI DIRITTI DEGLI INTERESSATI 21
2. GESTIONE DELLA CIRCOLAZIONE DELLE INFORMAZIONI IN AMBITO BANCARIO 22
3. GESTIONE DELL'ANALISI DEI RISCHI E LA VALUTAZIONE D'IMPATTO 22
4. GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (C.D. *DATA BREACHES*) 23
5. GESTIONE DEI CONTRATTI DI FORNITURA E DELLE TERZE PARTI 23
6. GESTIONE DEL REGISTRO DEI TRATTAMENTI 23
7. GESTIONE DELLA VIDEOSORVEGLIANZA 24
8. GESTIONE DELLE ATTIVITÀ DI MARKETING 25

A. MODALITA' DI GESTIONE DEL DOCUMENTO

SOCIETÀ EMITTENTE	IBL BANCA
TITOLO	POLICY DI GRUPPO IN MATERIA DI DATA PROTECTION
IDENTIFICAZIONE DEL DOCUMENTO	PPRI_PDP
TIPOLOGIA DEL DOCUMENTO	POLICY
PERIMETRO DI APPLICABILITÀ	CAPOGRUPPO IBL BANCA E BANCHE E SOCIETÀ DEL GRUPPO
REDATTORE	DIREZIONE OPERATIVA – SERVIZIO ORGANIZZAZIONE E GOVERNANCE
CONTRIBUTORE	DIREZIONE LEGALE – UFFICIO CONSULENZA LEGALE
VALIDATORE[1]	SERVIZIO COMPLIANCE E ANTIRICICLAGGIO SERVIZIO RISK MANAGEMENT
APPROVATORE	CONSIGLIO DI AMMINISTRAZIONE

[1] Per "validatore" si intendono le Funzioni di controllo di II livello indicate che svolgono le verifiche *ex ante* come disciplinato all'interno del Regolamento SNI.

B. PREMESSA

1. Scopo del documento

Il presente documento, denominato “Policy di Gruppo in materia di Data Protection” (di seguito anche “Policy”) ha lo scopo di individuare, per le Banche e le Società del Gruppo IBL Banca (di seguito anche “Gruppo”), i ruoli ed i compiti per una gestione della protezione dei dati personali che sia conforme alle prescrizioni normative dettate dal Regolamento UE 2016/679 – *Regolamento Generale sulla Protezione dei Dati* (di seguito anche “Regolamento GDPR” o “GDPR”), nonché dai Provvedimenti del Garante Privacy e del Comitato europeo per la protezione dei dati (già “Gruppo ex art. 29”) applicabili alla realtà operativa del Gruppo.

Il Gruppo IBL Banca si è dotato, altresì, della Policy di Gruppo in materia di Data Retention, con l’obiettivo di individuare le modalità di gestione della conservazione e minimizzazione dei dati personali oggetto di trattamento conformemente alle prescrizioni normative dettate dal Regolamento GDPR, e alla quale si rimanda per maggiori dettagli.

Inoltre, il Gruppo IBL Banca si è dotato della Policy di Gruppo in materia di metodologia per l’analisi dei rischi e Data Protection Impact Assessment (“DPIA”), al fine di fornire indicazioni circa l’approccio metodologico adottato dalla Capogruppo IBL Banca e dalle Banche/Società del Gruppo controllate per l’analisi dei rischi e la valutazione degli impatti per i trattamenti di dati personali che presentano un rischio elevato per i diritti e le libertà delle persone fisiche.

Altresì, ciascuna Banca/Società del Gruppo disciplina, in appositi manuali operativi, le attività, i controlli, i compiti e le responsabilità nella gestione della protezione dei dati personali, al fine di garantire la conformità alle prescrizioni normative vigenti.

2. Applicabilità

Le indicazioni contenute all’interno della presente Policy sono applicabili a tutte le Banche/Società[2] del Gruppo IBL Banca, previa approvazione del documento da parte del Consiglio di Amministrazione delle singole Banche/Società.

3. Riferimenti

Vengono di seguito indicati i principali riferimenti della presente Policy alla legge e in generale, a disposizioni normative (riferimenti esterni) e alla normativa interna del Gruppo (riferimenti interni).
Nel prosieguo del documento, per “Società” si intende ciascuna Banca e Società appartenente al Gruppo IBL Banca.

[2] Per la Società Moneytec le attività inerenti l’Area ICT sono gestite dalla struttura interna alla Società e le attività inerenti la parte Legale sono presidiate da soggetti esterni al Gruppo IBL, come specificato anche nelle successive sezioni del presente documento.

3.1. Riferimenti esterni

PROVVEDIMENTO	DESCRIZIONE
REGOLAMENTO UE 2016/679	REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DEL 27 APRILE 2016
PARERE GRUPPO DI LAVORO EX ART. 29[3]	LINEE GUIDA SUI RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI
PROVVEDIMENTO DEL GARANTE 27/05/2021	PROCEDURA TELEMATICA PER LA NOTIFICA DI VIOLAZIONI DI DATI PERSONALI (*DATA BREACH*)
PROVVEDIMENTO DEL GARANTE 12/09/2019	CODICE DI CONDOTTA PER I SISTEMI INFORMATIVI GESTITI DA SOGGETTI PRIVATI IN TEMA DI CREDITI AL CONSUMO, AFFIDABILITA' E PUNTUALITA' NEI PAGAMENTI
PROVVEDIMENTO DEL GARANTE 20/09/2012	APPLICABILITÀ ALLE PERSONE GIURIDICHE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI A SEGUITO DELLE MODIFICHE APPORTATE DAL D.L. N. 201/2011
PROVVEDIMENTO DEL GARANTE 12/05/2011	PRESCRIZIONI IN MATERIA DI CIRCOLAZIONE DELLE INFORMAZIONI IN AMBITO BANCARIO E DI TRACCIAMENTO DELLE OPERAZIONI BANCARIE
PRESCRIZIONI DEL GARANTE 19/01/2011	PRESCRIZIONI PER IL TRATTAMENTO DI DATI PERSONALI PER FINALITÀ DI MARKETING, MEDIANTE L'IMPIEGO DEL TELEFONO CON OPERATORE, A SEGUITO DELL'ISTITUZIONE DEL REGISTRO PUBBLICO DELLE OPPOSIZIONI
PROVVEDIMENTO DEL GARANTE 08/04/2010	PROVVEDIMENTO GENERALE SULLA VIDEOSORVEGLIANZA
PROVVEDIMENTO DEL GARANTE 27/11/2008	MISURE E ACCORGIMENTI PRESCRITTI AI TITOLARI DEI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI RELATIVAMENTE ALLE ATTRIBUZIONI DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA
PROVVEDIMENTO DEL GARANTE 13/10/2008	RIFIUTI DI APPARECCHIATURE ELETTRICHE ED ELETTRONICHE E MISURE DI SICUREZZA DEI DATI PERSONALI
PROVVEDIMENTO DEL GARANTE 25/10/2007	LINEE GUIDA PER I TRATTAMENTI DATI RELATIVI AL RAPPORTO SOCIETÀ-CLIENTELA
PROVVEDIMENTO DEL GARANTE 01/03/2007	LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET
PROVVEDIMENTO DEL GARANTE 23/11/2006	LINEE GUIDA PER IL TRATTAMENTO DI DATI DEI DIPENDENTI PRIVATI
PROVVEDIMENTO DEL GARANTE 27/10/2005	TRATTAMENTO DI ALCUNI DATI PERSONALI (IMMAGINI E IMPRONTE DIGITALI) DA PARTE DI BANCHE
PROVVEDIMENTO DEL GARANTE 27/10/2005	QUANDO IDENTIFICARE E FOTOCOPIARE I DOCUMENTI DI RICONOSCIMENTO DEI CLIENTI

[3] Il Gruppo, istituito dall'art. 29 della Direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Il Gruppo di Lavoro ex articolo 29, sarà sostituito a partire dal 25 maggio 2018 dal *Comitato europeo per la protezione dei dati*.

PROVVEDIMENTO	DESCRIZIONE
PRESCRIZIONE DEL GARANTE 30/11/2005	LICEITÀ, CORRETTEZZA E PERTINENZA NELL'ATTIVITÀ DI RECUPERO CREDITI
PROVVEDIMENTO DEL GARANTE 24/02/2005	"'FIDELITY CARD' E GARANZIE PER I CONSUMATORI. LE REGOLE DEL GARANTE PER I PROGRAMMI DI FIDELIZZAZIONE"

3.2. Riferimenti interni

DOCUMENTO	DESCRIZIONE
-	ORGANIGRAMMA E FUNZIONIGRAMMA AZIENDALE DELLE BANCHE/SOCIETÀ DEL GRUPPO IBL BANCA
MRUM_RRU	REGOLAMENTO DEL PERSONALE
PPRI_MADPIA	METODOLOGIA PER L'ANALISI DEI RISCHI E DPIA
MPRI_GAP	MANUALE OPERATIVO GESTIONE ADEMPIMENTI PRIVACY
RGOV_RCP	REGOLAMENTO DEL COMITATO DATA PROTECTION
PPRI_PDR	POLICY DI GRUPPO DATA RETENTION

4. Aggiornamenti

VERSIONE	DATA	DESCRIZIONE DELLE MODIFICHE
1.0	**09/05/2018**	NASCITA DEL DOCUMENTO
2.0	**13/04/2023**	AGGIORNAMENTO DEL DOCUMENTO PER REVISIONE ASSETTO DI GRUPPO

5. Glossario

TERMINE	DEFINIZIONE
ADDETTO AL TRATTAMENTO	L'Addetto al trattamento dei dati personali, il quale collabora con i Responsabili del trattamento, tratta i dati solo per gli scopi istituzionali, nello spirito della legge e secondo le istruzioni scritte che ha ricevuto; rispetta il segreto di ufficio e professionale, oltre che i requisiti di riservatezza e sicurezza durante l'uso dei dati personali; risponde per colpa grave o dolo specifico delle azioni che ha posto in essere nel trattamento di dati o per non aver rispettato le istruzioni impartite; segnala al Responsabile del trattamento interno eventuali anomalie o problemi che ha riscontrato nel corso della sua normale operatività.

TERMINE	DEFINIZIONE
AMMINISTRATORE DI SISTEMA	"Soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione" (ai sensi dell'art. 1, c. 1, lett. c, del D.P.R. n. 318/1999), ovvero quelle figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (gli amministratori di dati, gli amministratori di rete e di apparati di sicurezza e gli amministratori di sistemi *software* complessi possono essere equiparati a tale definizione).
AUTENTICAZIONE INFORMATICA	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.
AUTORIZZAZIONE	Il provvedimento adottato dal Garante con cui il Titolare del trattamento (ente pubblico, impresa, libero professionista) viene autorizzato a trattare determinati dati "sensibili" o giudiziari, ovvero a trasferire dati personali all'estero. In materia di dati sensibili e giudiziari, il Garante ha emanato alcune autorizzazioni generali che consentono a varie categorie di Titolari di trattare dati per gli scopi specificati senza dover chiedere singolarmente un'apposita autorizzazione al Garante.
SOCIETÀ DATI	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
BLOCCO	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.
CLIENTE	Qualsiasi soggetto, persona fisica o giuridica, che ha in essere un rapporto contrattuale o che intenda entrare in relazione con la Società.
COMUNICAZIONE	Il dare conoscenza dei dati personali a uno o più soggetti determinati, diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
CONSENSO	La libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi Titolare). È sufficiente che il consenso sia "documentato" in forma scritta (ossia annotato, trascritto, riportato dal Titolare o dal Responsabile o da un Addetto del trattamento su un registro o un atto o un verbale), a meno che il trattamento riguardi dati "sensibili"; in questo caso occorre il consenso rilasciato per iscritto dall'interessato (ad esempio con la sua sottoscrizione).
CONTRAENTE	Qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate.

TERMINE	DEFINIZIONE
CREDENZIALI DI AUTENTICAZIONE	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
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" (art. 4 punto 1, del GDPR).
DATA PROTECTION OFFICER (DPO)	Il soggetto nominato dal Titolare del trattamento in tutti i casi in cui le sue attività principali consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati. Nella traduzione italiana è il "Responsabile della protezione dei Dati".
DATI GIUDIZIARI	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
DATI IDENTIFICATIVI	I dati personali che permettono l'identificazione diretta dell'interessato.
DATI RELATIVI AL TRAFFICO	Qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione.
DATI RELATIVI ALL'UBICAZIONE	Ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico.
DATI PARTICOLARI (EX DATI SENSIBILI)	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
DATO ANONIMO	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
DATO PERSONALE	Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
DIFFUSIONE	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

TERMINE	DEFINIZIONE
DIRITTI DELL'INTERESSATO	I diritti riconosciuti all'interessato dagli artt. 15 - 22 del GDPR.
GARANTE	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR.
GDPR	Acronimo per *General Data Protection Regulation* (in italiano tradotto come *Regolamento Generale sulla Protezione dei Dati* – RGPD) che fa riferimento al Regolamento UE 2016/679.
GESTORE DI UN SISTEMA DI INFORMAZIONI CREDITIZIE	Il soggetto privato Titolare del trattamento dei dati personali registrati in un sistema di informazioni creditizie e che gestisce tale sistema stabilendone le modalità di funzionamento e di utilizzazione.
INFORMATIVA	Le informazioni che il Titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto quando i dati sono raccolti presso l'interessato stesso, oppure presso terzi. L'informativa deve precisare sinteticamente e in modo colloquiale quali sono gli scopi e le modalità del trattamento; se l'interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i diritti riconosciuti all'interessato; chi sono il Titolare e l'eventuale Responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, ecc.).
INTERESSATO	La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
LOCALE APERTO AL PUBBLICO O DIPENDENZA	Le succursali e qualunque locale adibito al ricevimento del pubblico per le trattative e la conclusione di contratti, anche se l'accesso è sottoposto a forme di controllo (ad es. negozi finanziari, uffici di rappresentanza, ecc.).
MISURE DI SICUREZZA	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
PAROLA CHIAVE	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

TERMINE	DEFINIZIONE
RESPONSABILE INTERNO DEL TRATTAMENTO	Il Responsabile interno del trattamento dei dati personali collabora con il DPO e con il Comitato Data Protection, ove previsto. Fornisce indicazioni/istruzioni operative agli Addetti al trattamento sulle modalità di trattamento e presidio dei dati personali e ne coordina le attività; cura le revisioni periodiche della mappatura dei trattamenti dati personali riferite alla propria area di competenza; garantisce la compliance alla normativa privacy nazionale ed europea; fornisce report puntuali al DPO sullo stato dell'applicazione della normativa; sorveglia e verifica l'operato degli Addetti al trattamento, ivi compresa la formazione del personale che partecipa ai trattamenti; verifica le esigenze privacy degli interessati in termini di richieste o a fronte di eventuali reclami; garantisce il presidio delle operazioni di trattamento nelle attività day-by-day.
RESPONSABILE ESTERNO DEL TRATTAMENTO	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (art. 4, paragrafo 8, GDPR).

6. Livello gerarchico

LIVELLO	DESCRIZIONE
III	POLICY

C. PARTE PRIMA - MODELLO ORGANIZZATIVO DATA PROTECTION

1. Ruoli e responsabilità

Di seguito si riportano i ruoli e le relative responsabilità degli Organi Sociali e delle principali Unità Organizzative delle Banche e Società del Gruppo IBL Banca, a vario titolo coinvolte nel perimetro della Policy in oggetto:

Capogruppo IBL Banca

- **Consiglio di Amministrazione**

  - definisce e approva le presenti politiche interne e gli indirizzi generali di Gruppo in materia di Data Protection;
  - designa e revoca il Data Protection Officer (DPO);
  - in caso di verifica ispettiva, indirizza le attività per far fronte alle richieste dell'Autorità Garante, coinvolgendo il DPO;
  - verifica l'operato dei Responsabili interni del trattamento, dei Responsabili esterni del trattamento ed eventuali richieste provenienti dal Garante per la protezione dei dati personali;

- **Comitato di Data Protection**

  - esprime pareri in merito alle questioni relative alla protezione dei dati personali;
  - ricopre una funzione di indirizzo all'interno della struttura organizzativa del Gruppo, raccogliendo le istanze e le richieste provenienti dai Responsabili del trattamento di dati personali;

- **Amministratore Delegato**

  - assicura l'applicazione della Policy e delle linee guida in essa contenute;

- **Direzione Operativa:**

  - per il tramite del Servizio Organizzazione e Governance e del Servizio Progetti Business e Crediti, ciascuno per gli ambiti di competenza, assicura la definizione delle modalità organizzative e dei presidi per la gestione e il trattamento dei dati personali[4];

[4] Relativamente alla Capogruppo IBL Banca e anche alle Società del Gruppo IBL Servicing, IBL Real Estate e IBL Assicura.

- per il tramite del Servizio Organizzazione e Governance, in linea con le responsabilità definite nella normativa interna, coordina l'aggiornamento del Registro dei Trattamenti[5] dei dati personali della Capogruppo e delle Società del Gruppo su input del DPO, dei Responsabili interni del trattamento, delle Funzioni di Controllo e/o a seguito di modifiche organizzative che impattano sui singoli trattamenti censiti nel Registro stesso;
- per il tramite del Servizio Organizzazione e Governance, e con il supporto delle strutture organizzative impattate, assicura la predisposizione e l'aggiornamento della normativa interna in materia Data Protection[6];
- per il tramite del Servizio ICT Management e Innovation gestisce[7], per il tramite dell'Ufficio Network e Infrastruttura e, in qualità di Amministratore di Sistema, di concerto con il Servizio Organizzazione e Governance e con l'Ufficio IT Governance e Sicurezza Informatica, tutti gli accessi alla rete e ai programmi definendo gli utenti e la scadenza delle password di accesso nel rispetto delle disposizioni interne della Capogruppo e delle Società del Gruppo e delle previsioni normative di legge (privacy);

Direzione Legale[8]

- garantisce il presidio delle tematiche in ambito privacy garantendo inoltre il coordinamento con il DPO per tutte le tematiche privacy rilevanti per le Società del Gruppo;
- gestisce, con il supporto delle strutture interne competenti, le richieste da parte degli interessati in relazione agli esercizi dei propri diritti fornendo riscontro agli stessi entro i termini previsti dalla normativa;
- riceve dai Responsabili esterni e/o dai Responsabili interni del trattamento le eventuali segnalazioni di *data breach* e, previa una valutazione preliminare, invia le stesse al DPO;
- in caso di *data breach*, coordina le attività da porre in essere per accertare la segnalazione ricevuta e, se necessario, convocare il Comitato Data Protection;
- garantisce l'aggiornamento delle informative privacy.

[5] Relativamente alla Capogruppo IBL Banca e anche alle Società del Gruppo IBL Servicing, IBL Real Estate, IBL Assicura e Moneytec.
[6] Relativamente alla Capogruppo IBL Banca e anche alle Società del Gruppo IBL Servicing, IBL Real Estate, IBL Assicura e Moneytec.
[7] Relativamente alla Capogruppo IBL Banca e anche alle Società del Gruppo IBL Servicing, IBL Real Estate e IBL Assicura.
[8] Relativamente alla Capogruppo IBL Banca e anche alle Società del Gruppo IBL Servicing, IBL Real Estate, IBL Assicura, Banca Capasso e Banca di Sconto.

Banche/Società del Gruppo[9]

Relativamente alle Banche/Società del Gruppo in perimetro, si riportano i ruoli e le responsabilità degli Organi Sociali e delle principali Unità Organizzative:

- **Consiglio di Amministrazione delle singole Banche/Società del Gruppo**
  - approva le presenti politiche interne in materia di Data Protection;
  - designa e revoca il Data Protection Officer (DPO);
  - in caso di verifica ispettiva, indirizza le attività per far fronte alle richieste dell'Autorità Garante coinvolgendo il DPO;
  - verifica l'operato dei Responsabili interni del trattamento, dei Responsabili esterni del trattamento ed eventuali richieste provenienti dal Garante per la protezione dei dati personali;

- **Amministratore Delegato delle singole Banche/Società del Gruppo**
  - assicura l'applicazione della Policy e delle linee guida in essa contenute;

- **Funzione Organizzazione e IT delle singole Banche**[10] **del Gruppo**
  - assicurano la definizione delle modalità organizzative per la gestione e il trattamento dei dati personali;
  - coordinano l'aggiornamento del Registro dei Trattamenti dei dati personali di Banca di Sconto e di Banca Capasso su input del DPO, dei Responsabili interni del trattamento, delle Funzioni di Controllo e/o a seguito di modifiche organizzative che impattano sui singoli trattamenti censiti nel Registro stesso.;
  - assicurano, con il supporto delle strutture organizzative impattate, la predisposizione e l'aggiornamento della normativa interna in materia Data Protection;
  - gestiscono gli accessi alla rete e ai programmi definendo gli utenti e la scadenza delle password di accesso nel rispetto delle disposizioni interne della Banca e del Gruppo e delle previsioni normative di legge (privacy).

Il Regolamento GDPR individua i soggetti preposti al trattamento dei dati personali, delineando le figure fondamentali. Di seguito si riportano i principali compiti e responsabilità attribuiti alle figure previste dal GDPR in coerenza con il modello definito dal Gruppo IBL Banca.

[9] Per la Società Moneytec le attività inerenti l'Area ICT sono gestite dalla struttura interna alla Società e le attività inerenti la parte Legale sono presidiate da soggetti esterni al Gruppo IBL, come specificato anche nelle successive sezioni del presente documento.
[10] Relativamente a Banca Capasso e Banca di Sconto.

1.1 Titolare del trattamento

Il Titolare del trattamento è definito, ai sensi dell'art. 4, paragrafo1, punto 7 del Regolamento GDPR, come "*la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità di trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*".

Il Titolare del trattamento è la Società nella sua interezza, rappresentata dall'Organo con Funzioni di Supervisione Strategica (Consiglio di Amministrazione della Società), che individua e revoca il Data Protection Officer e i soggetti, interni ed esterni, Responsabili del trattamento.

Il Titolare del trattamento può, inoltre, delegare specifiche attività all'Organo con Funzione di Gestione (Amministratore Delegato), chiedendo a quest'ultimo di relazionargli periodicamente sull'esercizio della propria delega, indipendentemente dalle responsabilità che restano in capo al Titolare stesso (cfr. art. 24 del GDPR).

Nello specifico, il Titolare del trattamento:

- in caso di violazioni per le quali la legge preveda sanzioni di carattere amministrativo a carico della Società, risponde per il danno cagionato dal suo trattamento, solo se non ha adempiuto agli obblighi previsti dal Regolamento UE 2016/679 o ha agito in modo difforme o contrario rispetto al Regolamento stesso;
- designa e revoca il Data Protection Officer (DPO), i Responsabili interni e i Responsabili esterni;
- in caso di verifica ispettiva, indirizza le attività per far fronte alle richieste dell'Autorità Garante coinvolgendo il DPO;
- gestisce, in collaborazione con il Comitato di Data Protection ove presente[11], e sentito il parere del DPO, la verifica dell'operato dei Responsabili interni, dei Responsabili esterni del trattamento ed eventuali richieste provenienti dal Garante Privacy;
- predispone e mantiene aggiornato il Registro dei trattamenti dei dati personali (cfr. art. 30 del GDPR).

Il Titolare del trattamento, sulla base di specifici atti di delibera procede a:

- attuare il Modello Organizzativo per la Data Protection;
- designare il DPO ed approvare l'atto che ne definisce i compiti e le responsabilità.

Al Titolare del trattamento, ai sensi dell'art. 24 del GDPR, è prescritto il dovere di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e

[11] Allo stato attuale soltanto la Capogruppo IBL Banca ha istituito il Comitato Data Protection.

gravità diverse per i diritti e le libertà delle persone fisiche. Ai sensi del paragrafo 2 dell'art. 24 del GDPR "*se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento*".

1.2 Comitato Data Protection

Al Comitato Data Protection della Capogruppo IBL Banca sono demandati compiti di coordinamento e di indirizzo in materia di protezione dei dati personali della Capogruppo stessa. Allo stato attuale soltanto la Capogruppo IBL Banca si è dotata di un Comitato Data Protection.

In particolare, al Comitato Data Protection, relativamente alla Capogruppo IBL Banca, spettano le seguenti responsabilità:

- fornire indicazioni e gestire le eventuali problematiche che si dovessero presentare in materia di Data Protection;
- riunirsi ad evento per la condivisione di tematiche con impatto sulla protezione dei dati personali trattati da parte della Banca;
- raccogliere le istanze e le richieste provenienti dai Responsabili interni del trattamento di dati personali (tra le quali rientrano, a titolo meramente esemplificativo, eventuali richieste provenienti dai Responsabili esterni del trattamento, che i Responsabili interni riportano al Comitato);
- stabilire le priorità e definire le tempistiche dei progetti con risvolti sul trattamento dei dati personali;
- supportare la Banca affinché sia garantito il rispetto dei principi della protezione dei dati fin dalla progettazione (c.d. privacy *by design*) e per impostazione predefinita (c.d. privacy *by default*);
- esprimere un parere non vincolante sulla valutazione d'impatto predisposta dai Responsabili interni del trattamento;
- approfondire e gestire eventuali *data breach*, in conformità a quanto previsto dalle procedure interne della Banca;
- promuovere le attività necessarie a garantire il rispetto della normativa in ambito privacy.

Al Comitato partecipano:

- Amministratore Delegato (Presidente del Comitato);
- Vice Direttore Generale CFO e Credit;
- Vice Direttore Generale Planning e Operations;
- Responsabile Direzione Operativa;
- Responsabile della Direzione Legale;

e tutte le strutture eventualmente coinvolte negli argomenti di Data Protection da analizzare (i.e. DPO, Responsabili interni del trattamento, ecc).

Per i dettagli sui componenti del Comitato e sul suo funzionamento si rimanda al *Regolamento Comitato Data Protection*.

1.3 Data Protection Officer

Il DPO (Data Protection Officer)[12] è il soggetto indipendente cui competono le responsabilità di supervisionare e garantire i trattamenti di dati personali ed è tempestivamente e adeguatamente coinvolto dal Titolare del trattamento in tutte le questioni riguardanti la protezione dei dati personali.

Al DPO spettano i seguenti compiti:

- sorvegliare l'attuazione e l'applicazione delle politiche in ambito Data Protection all'interno della Società e riferire al Titolare del trattamento in merito ad eventuali non conformità rilevate;
- applicare quanto richiesto dalla normativa con particolare riguardo ai requisiti concernenti la protezione dei dati (progettazione, informazione all'interessato);
- controllare che eventuali violazioni e/o *data breach* siano documentate, notificate e comunicate internamente;
- assumere, sentito il Titolare, il compito di punto di contatto per il Garante della Privacy nel caso di verifiche ispettive e verso gli interessati per l'esercizio dei loro diritti e/o per fornire informazioni;
- fornire pareri e supporto per gli ambiti di competenza in merito alla valutazione d'impatto e/o alla *data breach*;
- consultare il Garante Privacy nel caso in cui sia necessario sottoporgli quesiti o istanze di verifica.

Il DPO svolge, dunque, un ruolo centrale nel Modello Organizzativo di Data Protection e funge, nel contesto aziendale, da garante, funzione di vigilanza, indipendente ed autonoma. Non può svolgere attività operative o avere la responsabilità delle stesse; deve, pertanto, essere indipendente nello svolgimento delle attività di competenza.

A titolo esemplificativo, la Corte di Giustizia dell'Unione europea ha ritenuto sussistente un'incompatibilità tra il ruolo di DPO e quello di presidente del Consiglio aziendale, dal momento che potrebbe configurarsi un conflitto di interessi laddove il DPO venisse incaricato di altri compiti o funzioni che lo indurrebbero a determinare le finalità e i mezzi del trattamento dei dati personali, compromettendo così l'esercizio indipendente delle proprie funzioni (cfr. CGUE, sentenza C - 453/21 del 9 febbraio 2023).

Inoltre, anche il Garante ha evidenziato che l'indipendenza prescritta dal Considerando 97 del GDPR potrebbe venire meno allorché il DPO dovesse rivestire, all'interno dell'organizzazione dell'ente, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali (ad esempio perché contribuisce a definire le caratteristiche del trattamento *by design* e

[12] Il GDPR ha introdotto la figura del DPO, che deve essere nominato in tutti i casi in cui l'azienda Titolare svolge trattamenti che prevedano il controllo regolare e sistematico degli interessati, ovvero la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, specificandone compiti, ruolo e il suo posizionamento nell'organigramma aziendale in tre articoli: art. 37 (*Designazione del responsabile della protezione dei dati*), art. 38 (*Posizione del responsabile della protezione dei dati*) e art. 39 (*Compiti del responsabile della protezione dei dati*).
Inoltre, il Gruppo di Lavoro ex art. 29 (poi divenuto Comitato Europeo per la protezione dei dati) ha predisposto delle Linee guida (si veda *Linee guida sui responsabili della protezione dei dati)* emanate in data 5 aprile 2017.

by default, ovvero perché gli sono attribuiti potestà decisionali all'esito di trattamenti di dati personali di particolare delicatezza, cfr. Provvedimento del 29 aprile 2021, n. 186).

Nel Provvedimento menzionato sono indicate alcune situazioni di conflitto di interessi con il ruolo di DPO in relazione a ruoli manageriali di vertice quali, *inter alia*, responsabile finanziario, direzione risorse umane, responsabile IT, responsabile per la prevenzione della corruzione e per la trasparenza, responsabile dei sistemi informativi, ovvero quello dell'ufficio di statistica. In ogni caso, l'indagine deve essere effettuata "*caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento*".

Nello specifico, il DPO supporta, se necessario, la Direzione Legale della Capogruppo IBL Banca nella gestione delle richieste ricevute dagli interessati e verifica che le risposte all'interessato siano fornite nel rispetto delle tempistiche previste.

Supporta, altresì, la Direzione Legale della Capogruppo IBL Banca nella predisposizione e aggiornamento delle informative privacy.

In coerenza con quanto indicato nel Modello Organizzativo di Data Protection, il ruolo del DPO può essere assunto da un soggetto interno o esterno. Allo stato attuale, per il Gruppo IBL il ruolo di DPO è assunto da un soggetto esterno (tutte le Società del Gruppo, ivi compresa la Capogruppo, hanno il medesimo DPO). I dati di contatto del DPO sono comunicati al Garante Privacy e pubblicati sul sito internet della Società nella sezione dedicata alla protezione dei dati personali[13].

Il DPO rendiconta, annualmente, agli organi aziendali della Capogruppo IBL Banca e di ciascuna Società del Gruppo, le risultanze delle attività svolte e per le quali è stato coinvolto, in applicazione e osservanza delle disposizioni normative in ambito Data Protection. Il DPO predispone e sottopone agli organi aziendali una Relazione annuale sulle attività svolte nel periodo di riferimento.

1.4 Responsabile interno del trattamento

Il Titolare del trattamento, in relazione a quanto specificamente indicato nel Registro dei trattamenti, individua, per ciascuna tipologia di trattamento censito nel Registro, coloro che ricoprono il ruolo di "Responsabile interno del trattamento" tra i Responsabili di Direzione e Servizio delle singole unità organizzative della Società. I Responsabili ricevono specifiche istruzioni con indicazione dei trattamenti di dati assegnati, le finalità perseguite, la tipologia dei dati personali, gli obblighi e i diritti a loro assegnati.

Al Responsabile interno dei trattamenti spettano le seguenti attribuzioni:

- collaborare con il DPO e con il Comitato Data Protection, ove presente;
- fornire indicazioni/istruzioni operative agli Addetti al trattamento sulle modalità di trattamento e presidio dei dati personali, coordinandone le attività;

[13] Cfr. art. 37, par. 1, lettera 4 del GDPR.

- curare le revisioni periodiche del Registro dei trattamenti dati personali, relativamente ai trattamenti di propria competenza;
- riportare al DPO informazioni circa lo stato d'applicazione della normativa e/o eventuali violazioni di dati personali delle quali sia venuto a conoscenza;
- sorvegliare e verificare l'operato degli Addetti al trattamento, ivi compresa la formazione del personale che partecipa ai trattamenti dati di clienti, dipendenti, fornitori e/o partner commerciali;
- verificare la legittimità degli interessati in termini di esercizio dei loro diritti;
- garantire il presidio delle operazioni di trattamento dei dati personali nelle attività *day-by-day*;
- procedere, se indicato dal DPO, alla cancellazione dei dati su richiesta dell'interessato (cfr. Parte Seconda, par. 1 della presente Policy).

1.5 Responsabile esterno del trattamento

Il soggetto esterno che svolge un'attività per conto della Società e tratta dati personali la cui titolarità sia di quest'ultima, può assumere il ruolo di Responsabile esterno del trattamento ai sensi dell'art. 28, par.1 del GDPR[14]. Il Responsabile è designato dal Titolare del trattamento, mediante la sottoscrizione di uno specifico accordo tra le parti.

Nello specifico, il soggetto identificato dalla Società quale Responsabile esterno del trattamento ha il compito di:

- trattare i dati personali su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure di sicurezza richieste ai sensi dell'art. 32 del GDPR;
- assistere il Titolare del trattamento per dare seguito alle richieste di esercizio dei diritti da parte degli interessati;
- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di comunicazione delle violazioni di dati personali ai sensi degli artt. 33 e 34 del GDPR e/o delle valutazioni di impatto sulla protezione dei dati personali ai sensi degli artt. 35 e 36 del GDPR;
- su indicazione del Titolare del trattamento, cancellare o restituire tutti i dati personali al termine della prestazione dei servizi relativi al trattamento;
- consentire ad attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

[14] L'art. 28 par. 1 del GDPR recita: *"Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".*

I rapporti tra le parti e i rispettivi trattamenti sono disciplinati da un accordo stipulato tra le parti che vincola il Responsabile all'utilizzo dei dati personali nel rispetto degli obblighi riportati nel Data Protection Agreement sottoscritto ai sensi dell'art. 28, paragrafo 3 del GDPR.

1.6 Addetti al trattamento

Gli Addetti al trattamento sono coloro che, nel rispetto di quanto previsto dall'art. 29 del GDPR, utilizzano i dati personali per il compimento di operazioni di trattamento.

A tal fine gli Addetti ricevono specifiche istruzioni scritte per il tramite del Responsabile interno del trattamento con indicazione dell'ambito del trattamento cui sono autorizzati. Essi sono individuati tra i dipendenti ed eventualmente, i collaboratori interni e/o esterni di ciascuna Società del Gruppo.

Ciascun Addetto al trattamento è tenuto a seguire le istruzioni operative ricevute e le procedure predisposte per il governo della Data Protection.

In particolare, l'Addetto al trattamento ha le seguenti responsabilità:

- collaborare con i Responsabili interni del trattamento;
- trattare i dati solo per gli scopi istituzionali, secondo le istruzioni scritte ricevute e nel rispetto di quanto indicato nel Registro dei trattamenti;
- rispettare i requisiti di riservatezza e sicurezza durante l'uso dei dati personali;
- rispondere per colpa grave o dolo specifico delle azioni che ha posto in essere nel trattamento di dati o per non aver rispettato le istruzioni impartite;
- segnalare al Responsabile interno del trattamento eventuali anomalie o problemi che ha riscontrato nel corso della sua normale operatività.

1.6.1. Assunzione e formazione del personale

La Direzione Risorse Umane e Relazioni Istituzionali della Capogruppo consegna, nel momento dell'assunzione del dipendente, sia per la Capogruppo che per le Società controllate, la seguente documentazione:

- specifica informativa Privacy e, ove necessario, ne acquisisce il relativo consenso;
- lettera di assegnazione del dipendente alla specifica unità operativa;
- istruzioni operative "Addetto al trattamento dei dati personali".

La Direzione Risorse Umane e Relazioni Istituzionali della Capogruppo predispone il piano formativo annuale in tema di Data Protection per il personale dipendente delle Banche e Società del Gruppo coinvolto a qualsiasi titolo in attività di trattamento dei dati personali.

1.7 Amministratori di Sistema[15]

Gli Amministratori di Sistema sono coloro che, in linea con quanto previsto dal Provvedimento del Garante del 27 novembre 2008[16], provvedono alla gestione delle attività sui sistemi informatici aziendali utilizzati per il trattamento dei dati personali in termini di creazione dei profili di accesso, manutenzione e gestione e alla sicurezza logica.

Gli Amministratori di Sistema sono nominati con apposita lettera che ne definisce il ruolo, i compiti e le responsabilità.

Al riguardo è compito del Titolare del trattamento:

- individuare e nominare quei soggetti che possono svolgere la mansione di Amministratori di Sistema;
- aggiornare nel continuo l'elenco del personale nominato "Amministratore di Sistema";
- gestire i log di accesso ai sistemi in termini sia di requisiti di completezza, inalterabilità e possibilità di verifica della loro integrità, sia con specifica indicazione della temporalità e dell'evento che le ha generate. Tali log sono conservati per un periodo non inferiore a sei mesi.

Spetta, inoltre, al Titolare del trattamento verificare l'operato degli Amministratori di Sistema con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

[15] Per la Società Moneytec tale aspetto è presidiato dalla Società stessa e non dalla Capogruppo.

[16] Cfr. Provvedimento *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* e ss. mm.

D. PARTE SECONDA - I PRINCIPALI ADEMPIMENTI DATA PROTECTION

1. Gestione dei diritti degli interessati[17]

Il GDPR riconosce al soggetto a cui si riferiscono i dati trattati (ad esempio cliente, dipendente, fornitore, ecc.) una serie di diritti volti a permettergli un adeguato e diretto controllo sul rispetto da parte della Società dei limiti e delle condizioni poste al trattamento dei dati personali.

In tale contesto, gli artt. 7 e 15-22 del GDPR obbligano ciascuna Banca/Società appartenente al Gruppo, in qualità di Titolare del trattamento, a fornire idoneo riscontro alle richieste avanzate dagli interessati con riferimento ai dati personali che li riguardano.

Ai sensi del Considerando 7 del GDPR, gli interessati hanno il diritto di avere il controllo sui dati personali che li riguardano. Il GDPR attribuisce agli interessati i seguenti diritti, già sostanzialmente previsti dal D. Lgs. n. 196/2003 ("Codice Privacy") e, precisamente:

- diritto di revoca del consenso (art. 7, paragrafo 3);
- diritto all'informativa (artt. 13 - 14);
- diritto di accesso (art. 15);
- diritto di rettifica (art. 16);
- diritto alla cancellazione, con previsione del diritto all'oblio in relazione ai dati resi pubblici (art. 17);
- diritto alla limitazione del trattamento (art. 18);
- diritto alla portabilità dei dati (art. 20);
- diritto di opposizione (art. 21);
- diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione (art. 22).

Le richieste presentate ai sensi dei citati articoli comportano l'obbligo di verificare la presenza all'interno dei propri archivi e dei documenti effettivamente conservati dei dati personali relativi all'interessato oggetto della richiesta, quindi di procedere in base alla specifica richiesta ricevuta dall'interessato. Il riscontro all'interessato deve essere conciso, trasparente e facilmente accessibile, lo stesso deve essere fornito entro un mese, estensibile fino a tre mesi nelle ipotesi di particolare complessità, in forma scritta anche attraverso strumenti elettronici che ne favoriscano l´accessibilità e può essere dato oralmente solo se così richiede l´interessato stesso.

[17] Per la Società Moneytec tale aspetto è presidiato dalla Società stessa e non dalla Capogruppo.

2. Gestione della circolazione delle informazioni in ambito bancario

Il Garante Privacy ha emanato uno specifico Provvedimento in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie[18] riferite sia a quelle che comportano movimentazione di denaro, sia di sola consultazione (il c.d. inquiry) effettuate sui dati bancari riconducibili al singolo cliente. Le prescrizioni contenute nel Provvedimento si applicano alle Banche/Società del Gruppo IBL Banca.

Al riguardo ciascuna Banca/Società del Gruppo:

- implementa strumenti di alerting in grado di individuare comportamenti anomali o a rischio relativi a operazioni di inquiry e/o a movimentazioni di denaro;
- prevede specifiche attività di verifica periodica sulla corretta applicazione del Provvedimento;
- definisce specifiche modalità da adottare nel caso in cui siano stati accertati accessi indebiti da parte di soggetti non autorizzati per darne tempestiva comunicazione all'interessato e al Garante Privacy.

Si osserva inoltre che per questo tema ciascuna Banca/Società si avvale del supporto del proprio outsourcer informatico che, a sua volta, ha predisposto apposita documentazione per far fronte alle specifiche richieste del citato Provvedimento.

3. Gestione dell'analisi dei rischi e la valutazione d'impatto[19]

Ai sensi degli artt. 35 e 36, il GDPR impone l'obbligo per il Titolare del trattamento di procedere, ove necessario, ad un *Data Protection Impact Assessment*, ("DPIA") quando *"un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*.

Il Gruppo IBL si è dotato della Policy di Gruppo in materia di metodologia per l'analisi dei rischi e DPIA e Data Protection Impact Assessment[20], alla quale si rimanda per i dettagli, il processo di analisi dei rischi privacy e l'approccio metodologico per condurre la valutazione degli impatti per i trattamenti di dati personali che presentano un rischio elevato per i diritti e le libertà delle persone fisiche.

[18] Cfr. Provvedimento del Garante Privacy n. 192 del 12 maggio 2011 "*Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie"*

[19] Per la Società Moneytec tale aspetto è presidiato dalla Società stessa e non dalla Capogruppo.

[20] La metodologia utilizzata è coerente con quanto indicato dall'art. 5, paragrafo 2 (*Principi applicabili al trattamento di dati personali*), dall'art. 24 (*Responsabilità del titolare del trattamento*) e dai Considerando n. 74, n. 78 del GDPR, nonché dal documento WP248 rev. 0.1 – *Linee guida sulla DPIA* del 4 ottobre 2017 e dallo standard ISO/IEC 29134:2017 *Information technology -- Security techniques -- Guidelines for privacy impact assessment.*

4. Gestione delle violazioni di dati personali (c.d. *data breaches*)[21]

Ai sensi degli artt. 33 e 34, il GDPR impone l'obbligo per il Titolare del trattamento di gestire il processo di rilevazione, gestione e segnalazione delle violazioni (conosciute anche con il termine di *data breaches*[22]) che coinvolgono dati personali e le modalità attraverso cui sono effettuate le comunicazioni delle violazioni di dati personali al Garante Privacy e, ove necessario, ai soggetti coinvolti nella violazione (interessati).

Sono previsti diversi adempimenti in funzione del rischio che il *data breach* comporta per gli interessati e, in particolare:

- il Titolare notifica al Garante privacy solo i *data breaches* con rischio probabile per gli interessati, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza;
- il Titolare comunica agli interessati solo i *data breaches* con rischio elevato per gli stessi, senza ingiustificato ritardo dall'avvenuta conoscenza;
- il Titolare documenta tutti i *data breaches* (anche quelli non notificati), specificando circostanze, effetti e azioni correttive adottate, per consentire all'Autorità di verificare la *compliance* con il quadro normativo vigente.

Il Registro delle violazioni è aggiornato ad evento, ogni qualvolta si verifica una violazione dei dati personali da parte dell'Ufficio Consulenza Legale.

La notifica di una violazione dei dati personali all'Autorità di controllo deve contenere le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679, come previsto dal Provvedimento del Garante del 27 maggio 2021.

5. Gestione dei contratti di fornitura e delle terze parti[23]

Ai sensi dell'art. 28 il GDPR impone l'obbligo per il Titolare del trattamento di gestire le azioni da porre in essere nei confronti di quei soggetti terzi che si trovano a trattare informazioni personali la cui titolarità è attribuibile ad una Banca/Società del Gruppo.

6. Gestione del Registro dei trattamenti

Ai sensi dell'art. 30, il GDPR impone l'obbligo per il Titolare di censire tutti i trattamenti di dati personali, mappare le relative responsabilità e i sistemi informatici a supporto degli stessi, nonché

[21] Per la Società Moneytec tale aspetto è presidiato dalla Società stessa e non dalla Capogruppo.
[22] Per tali intendendosi una 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.
[23] Per la Società Moneytec tale aspetto è presidiato dalla Società stessa e non dalla Capogruppo.

definire i tempi di conservazione dei dati personali, per ciascuna tipologia di trattamento censito nel Registro dei trattamenti.

A tale scopo ciascuna Banca/Società appartenente al Gruppo formalizza, in un apposito Registro, tutti i trattamenti di dati personali effettuati presso le proprie Direzioni e/o strutture organizzative.

Il Registro è aggiornato nel continuo dalle Banche/Società del Gruppo IBL.

L'aggiornamento del Registro è coordinato:

- dal Servizio Organizzazione e Governance della Capogruppo per la Capogruppo IBL Banca e per le Società IBL Servicing, IBL Real Estate, IBL Assicura e Moneytec;
- dall'Area ICT e Organizzazione per Banca Capasso;
- dalla struttura Organizzazione di Banca di Sconto,

su input del Responsabile interno del trattamento, del DPO o delle Funzioni di Controllo, a seguito di aspetti emersi in sede di verifica e/o a seguito di modifiche organizzative che impattano sui singoli trattamenti censiti nel Registro.

7. Gestione della videosorveglianza

Il Garante Privacy ha emanato uno specifico Provvedimento in materia di videosorveglianza del 8 aprile 2010, che obbliga il Titolare del trattamento ad adottare una serie di azioni dedicate per dar seguito alle prescrizioni a carattere cogente in esso contenute. Le prescrizioni contenute nel Provvedimento si applicano alle sole Banche/Società del Gruppo IBL Banca dotate di sistemi di videosorveglianza.

A tale scopo ciascuna Banca/Società del Gruppo predispone apposita documentazione con la quale:

- provvede ad identificare un Responsabile interno delle attività di trattamento e gli Addetti al trattamento cui consegna specifiche istruzioni operative;
- identifica i soggetti/le società che effettuano la manutenzione/gestione degli impianti di videosorveglianza sottoponendogli, ove necessario, specifico Data Protection Agreement;
- predispone specifica informativa e la cartellonistica necessaria ad individuare correttamente la presenza di telecamere;
- stabilisce termini di conservazione delle immagini coerenti con le indicazioni del Provvedimento in applicazione del c.d. "*principio di proporzionalità*" e, comunque, per un periodo massimo di 5 giorni;
- implementa specifiche misure di sicurezza per regolamentare l'accesso alle immagini registrate, (i.e. "*doppia chiave*" fisica e logica che consente l'accesso alle immagini al solo personale individuato e autorizzato) in caso di necessità;
- sottoscrive accordi con le Rappresentanze Sindacali ai sensi dell'art. 4 della Legge n. 300/70 (c.d. "Statuto dei lavoratori").

8. Gestione delle attività di marketing[24]

Il Servizio Marketing e Advertising di Gruppo è responsabile delle attività di marketing per tutte le Società appartenenti al Gruppo.

I dati per finalità di marketing sono raccolti:

- direttamente presso l'interessato, nella sua qualità di cliente o potenziale cliente;
- tramite i canali web attraverso i form online presenti sui vari siti;
- tramite acquisizione di liste di contatti da fornitori esterni.

Nel caso in cui i dati vengano acquistati da altri soggetti (i.e. società di *direct marketing*, società che vendono liste od elenchi di nominativi e indirizzi postali, ecc.), è cura del Responsabile interno del trattamento del Servizio Marketing e Advertising di Gruppo, sentito anche il parere del DPO:

- verificare la fonte dei dati personali (i.e. da dove il fornitore abbia acquisito le informazioni con la data del loro aggiornamento);
- verificare le procedure seguite in relazione all'assolvimento degli obblighi di informativa e di acquisizione del consenso degli interessati;
- procedere al controllo sia della modulistica utilizzata sia della verifica dell'effettivo rilascio del consenso per finalità di marketing su un campione di soggetti che sia numericamente significativo rispetto al totale della lista;
- richiedere, se ritenuto opportuno, il rilascio di apposita dichiarazione a livello contrattuale sulle modalità seguite per garantire la conformità alle norme applicabili in materia di data protection (GDPR, Codice Privacy, Provvedimenti del Garante Privacy, Pareri espressi dal Gruppo di Lavoro ex art. 29).

Nel caso di dati personali che siano stati raccolti direttamente dall'interessato (ad esempio, cliente o potenziale cliente), l'utilizzo per fini di marketing (ivi compresi, a titolo esemplificativo scopi commerciali, promozionali, pubblicitari) può avvenire solo se:

- è stata fornita una preventiva e idonea informativa nella quale devono essere riportati tutti gli elementi previsti dall'art. 13 del GDPR;
- è stato acquisito uno specifico e separato consenso per l'utilizzo di tali dati per finalità di marketing da parte della Società, nonché per l'eventuale comunicazione dei dati a soggetti terzi.

Con riferimento all'informativa privacy, predisposta dall'Ufficio Consulenza Legale della Capogruppo per tutte le Banche e Società del Gruppo, ai sensi dell'art. 13 del GDPR, è necessario che siano specificati i seguenti aspetti:

[24] Per la Società Moneytec tale aspetto è presidiato dalla Società stessa e non dalla Capogruppo.

- le singole finalità del trattamento, rispetto a quelle connesse alla gestione del rapporto con l'interessato, per scopi di commercializzazione di prodotti e servizi (es. indagini di mercato, comunicazioni commerciali per lettera, materiale pubblicitario, ecc.);
- la natura facoltativa del conferimento dei dati per finalità di marketing e l'assenza di conseguenze sui rapporti in essere in caso di mancato rilascio dei dati da parte della clientela per tali finalità;
- l'eventuale comunicazione o cessione dei dati a terzi per le suddette finalità (indicando, nel caso, le categorie di soggetti destinatari);
- le modalità del trattamento dei dati, evidenziando l'eventuale utilizzo di particolari sistemi di organizzazione, raffronto ed elaborazione dei dati;
- l'esistenza del diritto per l'interessato di chiedere al titolare del trattamento l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento che lo riguardano e/o di opporsi al trattamento stesso;
- i tempi di conservazione dei dati personali;
- l'eventuale trasferimento di dati verso paesi non appartenenti allo Spazio Economico Europeo (SEE);
- i riferimenti del DPO e delle modalità attraverso le quali sono esercitabili i diritti previsti dagli artt. 7 e 15-22 del GDPR.

Per quanto riguarda il consenso, ai sensi dell'art. 7 del GDPR quest'ultimo deve essere *"informato, specifico, libero, e inequivocabile"* e deve risultare da una manifestazione esplicita dell'interessato differenziata in base alla specifica finalità di trattamento svolta.

Con riferimento all'utilizzo per fini commerciali di dati personali di clienti o potenziali clienti raccolti per il tramite di siti web appartenenti alle Società del Gruppo, restano fermi i principi della preventiva informativa e dell'acquisizione dello specifico consenso in mancanza del quale non è lecito l'utilizzo per fini di marketing.