GRUPPO CASSA CENTRALE
CREDITO COOPERATIVO ITALIANO

REGOLAMENTO DI GRUPPO

PER IL TRATTAMENTO DI DATI PERSONALI

Fonte Normativa: Regolamento

Approvato dal Consiglio di Amministrazione

Data della Delibera: 20 gennaio 2021

Owner	Autore
DPO	Servizio Data Protection

Destinatari
Capogruppo e Società del Gruppo

N° Versione	Data di approvazione in CdA di Capogruppo	Note
1	20 gennaio 2021	Aggiornamento del precedente Regolamento privacy in vigore prima della costituzione del gruppo bancario.

1. Sommario

1. Glossario

Banca/Banche affiliata/e: singolarmente ovvero collettivamente le Banche di Credito Cooperativo, le Casse Rurali e/o le Casse Raiffeisen aderenti al Gruppo Bancario Cooperativo, in quanto soggette all'attività di direzione e coordinamento da parte della Capogruppo in virtù della sottoscrizione del Contratto di Coesione.

Capogruppo: Cassa Centrale Banca – Credito Cooperativo Italiano S.p.A. in qualità di Capogruppo del Gruppo Bancario Cooperativo.

Categorie particolari di Dati personali: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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 – articolo 9 GDPR.

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 – articolo 4, punto 1), GDPR.

Data Protection Officer o DPO: il soggetto designato dal Titolare del trattamento per assolvere funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR.

Garante: l'Autorità garante italiana per la protezione dei Dati personali.

GDPR: il Regolamento UE 2016/679 in materia di protezione dei dati personali.

Gruppo: Gruppo Cassa Centrale – Credito Cooperativo Italiano.

Informativa: il documento con il quale il titolare del trattamento, in forma scritta o orale, informa il soggetto interessato circa le finalità e le modalità del trattamento medesimo.

Interessato: la persona fisica cui si riferiscono i dati personali oggetto di trattamento.

Referente privacy: il soggetto interno alla realtà aziendale del Titolare che supporta il DPO nello svolgimento delle sue funzioni.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati personali per conto del Titolare del trattamento o, eventualmente, di altro Responsabile del trattamento.

Soggetto autorizzato o Soggetto designato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile.

Società del Gruppo/Società: le Banche affiliate, le società da queste controllate, direttamente o indirettamente, e le altre Banche, Società prodotto, Società finanziarie, Società servizi e strumentali controllate, direttamente e/o indirettamente, dalla Capogruppo.

Titolare del trattamento: 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 del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati personali o insiemi di Dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione – articolo 4, punto 2), GDPR.

2. Premessa

Il presente Regolamento illustra le modalità di trattamento dei dati adottate da ogni singola Banca/Società, in applicazione della normativa vigente in materia di protezione dei dati personali, con particolare riferimento al Regolamento (UE) 2016/679 (c.d. "GDPR") ed al D. Lgs. 196/2003 così come novellato dal D. Lgs. 101/2018 e seguenti modifiche.

2.1. OBIETTIVI DEL DOCUMENTO

In coerenza con le esigenze di Cassa Centrale Banca e del relativo ruolo di Capogruppo e di Banca, il presente Regolamento ha l'obiettivo di definire le istruzioni alle quali si devono attenere tutte i soggetti che a vario titolo trattano dati personali per contro di ciascuna Banca e Società del Gruppo.

In particolare, in coerenza con le esigenze di Cassa Centrale Banca e del relativo ruolo di Capogruppo e di Banca, le disposizioni mirano a garantire che ogni trattamento di dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche, con specifico riferimento alla riservatezza ed all'identità personale di clienti, fornitori, dipendenti e tutti coloro che, più in generale, intrattengono rapporti con il Gruppo.

Chiunque si trovi a dover trattare dati personali per conto del Gruppo (a titolo esemplificativo ma non esaustivo: dipendenti, collaboratori, amministratori, sindaci, consulenti, ecc…) è tenuto al rispetto delle disposizioni descritte nel seguito al fine di garantire che ciascun trattamento di dati sia legittimo, lecito e svolto nel rispetto di tutti i presupposti normativi.

Nel caso in cui dovessero insorgere dei dubbi sull'applicazione del contenuto del presente documento, è possibile consultare il Referente Privacy e il DPO al fine di verificare congiuntamente la migliore soluzione applicabile al caso concreto.

2.2. ADOZIONE, AGGIORNAMENTO E DIFFUSIONE DEL DOCUMENTO

Il presente Regolamento, e i suoi relativi aggiornamenti, sono approvati dal Consiglio di Amministrazione della Capogruppo.

Il Regolamento, che si applica a tutte le Società del Gruppo, è trasmesso alle stesse per recepimento e relativa attuazione.

Al fine di assicurare a tutti i destinatari la conoscenza dei principi, degli indirizzi e delle procedure adottati dal Gruppo, il documento ed i relativi aggiornamenti sono portati a conoscenza degli stessi con le consuete modalità in uso alla Banca.

2.3. CONTESTO NORMATIVO DI RIFERIMENTO

Le fonti normative alle quali fa riferimento il presente documento sono:

- Il Codice Privacy come novellato dal D. Lgs. n. 101/2018;
- Il Regolamento europeo 2016/679;
- Il Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti – Provvedimento del Garante Privacy n. 163 del 12 settembre 2019;
- Linee guida sul trattamento dei dati personali attraverso dispositivi video n. 3/2019 dell'EDPB;
- Il Provvedimento del Garante Privacy n. 146 del 5 giugno 2019 recante le "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101";
- Il Provvedimento del Garante per la Protezione dei dati personali n. 229 dell'8 maggio 2014 denominato "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie";
- Provvedimento del Garante Privacy in materia di videosorveglianza dell'8 aprile 2010;
- Il Provvedimento del Garante per la Protezione dei dati personali n. 229 dell'8 aprile 2009 denominato "Prescrizioni in materia di operazioni di fusione e scissione fra società";
- Le Linee guida del Garante Privacy per i trattamenti dei dati relativi al rapporto banca-clientela rese note con Deliberazione n. 53 del 25 ottobre 2007;
- Il Provvedimento del Garante Privacy del 18 gennaio 2007 relativo a "Cessione in blocco e cartolarizzazione dei crediti".

Il presente documento integra e si coordina con la normativa interna adottata dal Gruppo, con particolare riferimento a:

- Policy per la protezione dei dati;
- Procedura per la gestione dei diritti degli interessati;
- Procedura per la gestione dei processi di Privacy by design e by default;
- Procedura per la gestione delle nomine;
- Procedura per la gestione delle violazioni dei dati personali (Data Breach).

3. Ruoli e responsabilità della Capogruppo

Di seguito si riporta il dettaglio, in termini di ruoli e responsabilità, degli Organi e delle Strutture della Capogruppo coinvolti nell'attuazione del presente Regolamento.

3.1. CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione si occupa di:

- approvare, il presente Regolamento e i successivi aggiornamenti;
- assumere la generale responsabilità di indirizzo e controllo in tema di trattamento dei dati personali;
- definire i mezzi e le risorse necessarie a presidiare e gestire gli aspetti di Data Protection;

3.2. DATA PROTECTION OFFICER (DPO)

Il GDPR attribuisce al DPO compiti di consulenza, informazione e sorveglianza, nonché un ruolo di contatto con il Garante e gli interessati, ammettendo la possibilità che gli siano attribuite mansioni ulteriori, purché non diano adito a conflitti di interesse.

In conformità al GDPR, il DPO è incaricato almeno dei seguenti compiti:

- **verificare nel continuo il rispetto della normativa** interna ed esterna in materia di protezione dei dati personali, mediante richiesta di documenti e/o accesso a tutte le banche dati contenenti informazioni utili all'espletamento dei propri compiti;

- **informare e fornire consulenza** in merito agli obblighi derivanti dal GDPR nonché dall'ulteriore normativa in materia di protezione dei dati personali;

- **fornire supporto e pareri** agli organi aziendali e agli autorizzati al trattamento in merito all'interpretazione della normativa interna ed esterna in materia di protezione dei dati personali e alle corrette modalità di trattamento dei dati personali;

- **sorvegliare l'osservanza** del Regolamento e di altre disposizioni legislative relative alla protezione dei dati, compresa l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, informando il CdA sulle criticità rilevate in materia di protezione dei dati;

- **svolgere**, nel continuo, attività di monitoraggio sulla DPIA, coinvolgendo le funzioni incaricate per i rispettivi ambiti di competenza e rilasciare gli opportuni pareri;
- **cooperare con il Garante**;
- **monitorare l'evoluzione della normativa** e informare il Titolare in merito alla necessità di aggiornamenti della documentazione privacy e della normativa interna che si rendano necessari alla luce di tali evoluzioni normative;
- **raccogliere** dalle singole unità organizzative competenti **le segnalazioni** in merito alla necessità di aggiornamento della normativa interna;
- **proporre al Consiglio di Amministrazione** l'aggiornamento della normativa interna in materia di protezione dei dati personali alla luce del complessivo livello di conformità alla normativa tempo per tempo applicabile in materia;
- **coordinare e gestire i flussi informativi** in ambito privacy all'interno della struttura organizzativa del Titolare;
- **fungere da punto di contatto** con gli interessati e il Garante per questioni connesse al trattamento di dati personali, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento dei dati personali, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

4. Ruoli e responsabilità delle Banche affiliate/Società del Gruppo

Di seguito si riporta il dettaglio, in termini di ruoli e responsabilità, degli Organi e delle Strutture delle Banche affiliate/Società del Gruppo coinvolti nel processo.

4.1. CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione si occupa di recepire e attuare tempestivamente il presente Regolamento e adeguare corrispondentemente il proprio corpus normativo.

4.2. REFERENTE PRIVACY

Il Referente Privacy ha il compito di essere la figura di raccordo tra il DPO e la propria realtà, in particolare sono a lui attribuite almeno le seguenti mansioni:

- **esaminare la normativa** in materia di protezione dei dati nonché gli aggiornamenti segnalati dal DPO e, laddove necessario, segnalare le istruzioni del DPO alle funzioni coinvolte;
- **curare l'implementazione della documentazione e della normativa interna** in materia di privacy e aggiornare il Registro dei trattamenti del Titolare, assicurando che tutta la documentazione sia sempre completa e aggiornata;
- **fornire consulenza** in materia di Data Protection, organizzare corsi di formazione per i colleghi e partecipare attivamente allo svolgimento delle analisi di privacy by design e DPIA assicurando il rispetto della metodologia prestabilita;
- **gestire le richieste di esercizio dei diritti degli interessati** e coadiuvare le funzioni competenti laddove necessario;
- **sovrintendere il processo di selezione e nomina dei responsabili** esterni, anche effettuando verifiche periodiche sugli stessi e **assicurare che tutto il personale** che tratta dati personali **sia stato appositamente designato autorizzato al trattamento**;
- **gestire eventuali Data Breach** e segnalare al DPO i casi più complicati;
- **garantire un flusso costante con il DPO**, da un lato attuando ogni comunicazione del DPO e portando in Consiglio di Amministrazione le relazioni/evidenze segnalate dal DPO stesso e dall'altro informando il DPO sulle criticità in materia di Data Protection, anche attraverso la predisposizione di report periodici.

5. Istruzioni ai Soggetti autorizzati

Ciascun soggetto autorizzato al trattamento di dati personali deve ricevere un apposito documento di designazione che lo autorizza a trattare dati personali per conto della Banca o Società del Gruppo, nonché tutte le opportune istruzioni per lo svolgimento del trattamento di dati personali.

Tali soggetti sono autorizzati ad eseguire operazioni di trattamento in relazione ai soli dati e per le sole finalità che risultano indispensabili allo svolgimento delle mansioni loro assegnate.

Non è pertanto consentito accedere indistintamente alla totalità dei dati e neppure compiere trattamenti eccedenti rispetto a quelli di competenza.

Tutti, inoltre, sono tenuti ad operare con la massima diligenza e attenzione in ciascuna fase di trattamento, dall'esatta acquisizione dei dati all'eventuale modifica degli stessi, nonché nei casi di cancellazione dei dati, nel rispetto delle disposizioni previste per ciascun trattamento.

5.1 MODALITÀ DI TRATTAMENTO E RISERVATEZZA

Il personale autorizzato deve mantenere il riserbo sulle informazioni utilizzate.

Al fine di evitare comunicazioni indebite, tutte le persone autorizzate al trattamento di dati personali:

- osservano le istruzioni impartite, evitando telefonate o colloqui effettuati indebitamente ad alta voce in presenza di terzi;
- si astengono dal comunicare informazioni a terzi che non siano in alcun modo autorizzati dall'Interessato, come, ad esempio, nei confronti:
  - del coniuge o convivente, cui venga consegnata documentazione bancaria riferita esclusivamente all'altro;
  - di familiari, contattati talora telefonicamente per comunicazioni dirette ai clienti, ma il cui contenuto venga invece rivelato ingiustificatamente ai primi;
  - di professionisti o soggetti legati da un rapporto di lavoro con l'Interessato;
  - di terzi che, per errore nell'imbustamento o nella spedizione della corrispondenza, divengano destinatari di comunicazioni scritte aventi ad oggetto informazioni bancarie (ad esempio, di estratti conto);
- si astengono dal comunicare informazioni presso recapiti non autorizzati, in modo da consentire a terzi di venire a conoscenza di dati riferiti all'Interessato (ad esempio, in caso di comunicazioni via mail o fax);
- più in generale, osservano le misure di sicurezza stabilite dal Gruppo.

Sono invece dovute e autorizzate le comunicazioni per adempiere a obblighi di legge o esecuzione degli impegni contrattuali nel limite strettamente necessario per adempiere a tali obblighi e meglio specificate nel successivo **paragrafo 5.3**.

Anche al fine di evitare il verificarsi di casi di Data Breach dovuti od omonimia o comunque allo scambio di identità, l'onere di identificare l'Interessato ricade sul Titolare possono essere utilizzati, oltre a idonei elementi di valutazione (quali la conoscenza personale o un'eventuale documentazione previamente acquisita, per esempio all'atto dell'instaurazione del rapporto), la richiesta della data di nascita o i dati personali degli Interessati contenuti in un documento di riconoscimento la cui esibizione è sempre richiesta.

Per particolari ordini e istruzioni della clientela può essere registrato il contenuto di conversazioni telefoniche intercorse, anche per eventuali profili di prova e di tutela di diritti in caso di controversia. In tutti questi casi, l'Interessato deve essere informato in ordine a tali registrazioni ai sensi dell'art. 13 del GDPR, in sede di conclusione del contratto o, al più tardi, all'inizio della prima conversazione telefonica. Per le registrazioni e gli eventuali dati personali connessi, se conservati, devono essere adottate le misure di sicurezza volte a prevenirne l'accesso, l'alterazione o l'uso non consentito da parte di soggetti non legittimati; il contenuto delle conversazioni non deve essere conservato per un tempo superiore a quello necessario per conseguire le finalità per le quali la registrazione è stata effettuata.

5.2 TUTELA DEI PROPRI DIRITTI

La Società può utilizzare in sede giudiziaria informazioni relative ai rapporti intrattenuti con la clientela per tutelare i propri diritti nelle controversie con gli Interessati.
I dati che possono essere prodotti in giudizio devono essere solo quelli pertinenti all'esigenza di far valere o difendere un diritto della Società; si deve evitare, pertanto, l'ingiustificata produzione di tabulati (ad es. interi estratti conto) contenenti dati personali non rilevanti per le citate finalità di difesa.

5.3 COMUNICAZIONE DEI DATI PER OBBLIGHI NORMATIVI

Laddove vi siano obblighi normativi che lo impongo la comunicazione dei dati personali è sempre consentita. A titolo esemplificativo sono autorizzate le seguenti comunicazioni:

- comunicazioni di informazioni personali per attuare la disciplina in materia di contrasto del riciclaggio e del terrorismo;
- comunicazioni di informazioni personali per l'accertamento e la repressione di violazioni tributarie, nei limiti previsti dalla legge;
- comunicazioni di informazioni, in conformità alla disciplina che regola la materia, alla Centrale Rischi della Banca d'Italia e alla Centrale d'Allarme Interbancaria;

- comunicazioni (nelle forme previste dalla legge) nei confronti dell'autorità giudiziaria e, nell'ambito di una procedura esecutiva, al creditore procedente nel rispetto delle vigenti disposizioni in materia di pignoramento presso terzi;
- comunicazioni a seguito di istanza di accesso alla documentazione bancaria ai sensi dell'art. 119 del Testo Unico delle leggi in materia bancaria e creditizia (D. Lgs. 1° settembre 1993, n. 385).

Deve, altresì, trovare corretta attuazione la prassi interbancaria del c.d. benefondi che prevede, nell'ambito della negoziazione di assegni tra banche per la realizzazione del credito portato dal titolo, la comunicazione dell'esistenza di una provvista sufficiente in relazione al pagamento di assegni da addebitare sul conto corrente del traente. Pertanto, le informazioni devono essere fornite ai soli soggetti legittimati all'incasso o alla negoziazione dell'assegno e non a terzi non autorizzati; inoltre, le informazioni fornite dalla Banca devono essere esatte, aggiornate e non eccedenti rispetto allo scopo per il quale il benefondi è utilizzato, che è relativo alla semplice informazione dell'esistenza o meno sul conto corrente del cliente della banca trattaria dei fondi necessari al pagamento dell'assegno.

5.4 TRASFERIMENTO DEI DATI ALL'ESTERO

Nel caso in cui il titolare del trattamento non ritenga di svolgere in autonomia un determinato trattamento può affidarlo interamente o in parte ad un soggetto terzo.
Nel caso di trasferimento di dati personali fuori dall'Italia, è necessario comprendere se i dati sono comunicati all'interno dell'Unione europea oppure no.
Nel caso di trasferimento di dati a un paese appartenente allo Spazio Economico Europeo (SEE, ossia UE + Norvegia, Liechtenstein, Islanda), non vi sono limitazioni, né ostacoli alla libera circolazione dei dati personali nell'Unione europea per motivi attinenti alla protezione dei dati (articolo 1, paragrafo 3 del GDPR).

I trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo o verso un'organizzazione internazionale sono consentiti a condizione che l'adeguatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 del GDPR).

In assenza di tale decisione, il trasferimento è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso

effettivi per gli interessati (art. 46 del GDPR). In assenza di ogni altro presupposto, è possibile trasferire i dati personali in base ad alcune deroghe previste dall'art. 49 del GDPR.

6.Informativa agli interessati

Ai sensi degli articoli 13 e 14 del Regolamento EU 2016/679, il titolare del trattamento è obbligato a fornire all'interessato determinate informazioni circa i trattamenti di dati personali che effettua, tali indicazioni sono contenute nell'informativa.

Spetta al Servizio Data Protection provvedere alla stesura delle informative privacy.

Il contenuto e le modalità di consegna delle informative sono diversi a seconda dei trattamenti effettuati e della categoria di interessati alle quali si rivolgono. Nel seguito le indicazioni da rispettare per ciascuna casistica.

6.1 INFORMATIVA A CANDIDATI E DIPENDENTI

Nel percorso di selezione e assunzione del personale vi sono diverse fasi, ognuna delle quali caratterizzata da specifiche dinamiche anche sotto l'aspetto relativo alla protezione dei dati.

6.1.1 RICEZIONE DI CURRICULUM SPONTANEO

Con riferimento a quanto prescritto dall'articolo 111-bis del Codice Privacy e dal Garante per la protezione dei dati, nei casi di ricezione di un curriculum spontaneamente trasmesso dall'interessato ad una delle società del Gruppo, l'informativa viene fornita al candidato nel momento del primo contatto utile successivo all'invio del curriculum stesso.
Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non è dovuto.

I dati ricevuti dal candidato possono essere utilizzati solo per i fini strettamente necessari al processo di selezione.

6.1.2 RICEZIONE DI CURRICULUM A SEGUITO DELLA PUBBLICAZIONE DI UN ANNUNCIO

Nei casi di ricezione di un curriculum a seguito di pubblicazione di annuncio, l'informativa deve essere fornita contestualmente alla pubblicazione dell'annuncio sul sito internet e/o a mezzo stampa, anche in forma sintetica e/o con rimandi ad un sito internet nel quale trovare l'informativa completa.

In ogni caso, l'informativa, se non fornita in precedenza, deve essere fornita al primo contatto utile.

6.1.3 ASSUNZIONE DIPENDENTE

Nei casi in cui venga assunta una nuova risorsa, l'Ufficio deputato (es. Gestione Risorse Umane) consegna al dipendente apposita informativa sul trattamento dei propri dati personali.

Per il personale che tratta dati personali, oltre alla consegna dell'informativa è necessario consegnare al dipendente anche la lettera con la quale lo stesso viene autorizzato al trattamento di dati personali per conto della banca o società del Gruppo.

L'ultima versione aggiornata dell'informativa dipendenti deve, inoltre, essere reperibile facilmente da ogni dipendente tramite pubblicazione nella intranet o nella bacheca aziendale.

6.2 COLLABORAZIONE ESTERNA

Nei casi in cui venga stipulato un accordo di collaborazione con persone fisiche, nella qualità di fornitori, consulenti o collaboratori, l'apposita informativa per i collaboratori viene rilasciata dal personale incaricato della raccolta dei dati personali contestualmente all'instaurazione del rapporto di collaborazione.

Ove previsto all'interno dei moduli, la U.O. competente raccoglie apposita sottoscrizione dell'Interessato per presa visione dell'informativa, da archiviare unitamente alla documentazione relativa al rapporto instaurato con lo stesso.

Laddove si tratti di collaborazioni con persone giuridiche non è necessario consegnare l'informativa.

6.3 INFORMATIVA VIDEOSORVEGLIANZA

I soggetti ripresi devono essere a conoscenza del fatto che la videosorveglianza è in funzione e per tale ragione è necessario garantire che gli interessati siano adeguatamente informati.

Al fine di informare gli interessati, sono predisposte le cosiddette informazioni di "primo livello" che consistono in un segnale di avvertimento che mostra, in modo comprensibile e chiaramente leggibile, che si stà per accedere ad una zona videosorvegliata e l'avviso inerente il conseguente trattamento dei dati. L'informativa breve deve contenere, tra le altre, il rinvio a dove è possibile reperire il testo completo contenente tutti gli elementi di cui all´art. 13 del Regolamento (sito internet, bacheca, ecc…).

Le informazioni devono essere posizionate ad una distanza ragionevole dai luoghi monitorati e devono essere presenti prima dei varchi mediante i quali si accede alle aree aziendali oggetto di ripresa. L'obiettivo, infatti, è quello di consentire ai soggetti di stimare quale area è oggetto di videosorveglianza al fine di determinare autonomamente se essere ripresi o meno.

Sono, inoltre, predisposte le c.d. informazioni di "secondo livello", le quali sono disponibili in luoghi facilmente accessibili all'interessato e consistono in un'informativa privacy più dettagliata, disponibile in posizioni centrali (ad es. ingresso, reception, scrivania cassiere) e/o mediante affissione su una parete e/o pubblicazione sul sito internet. Tale informativa di secondo livello è destinata a tutti i soggetti che potenzialmente o direttamente possono essere ripresi dai sistemi di videosorveglianza ed è finalizzata ad informare gli interessati in merito all'uso dei dati raccolti per mezzo del sistema di videoriprese.

6.4 INFORMATIVA ALLA CLIENTELA

La consegna dell'informativa ai clienti e la raccolta dei relativi consensi è posta in capo al Titolare per il tramite dei soggetti autorizzati addetti alla raccolta dei dati personali.

Prima del conferimento dei dati è necessario consegnare all'interessato l'apposita informativa sull'utilizzo dei propri dati personali da parte del Titolare del trattamento.

L'informativa deve essere consegnata in corrispondenza della registrazione dei dati in anagrafica o su apposito supporto e viene consegnata una tantum e non in relazione ad ogni singolo prodotto sottoscritto dal cliente.

Nei casi espressamente previsti, si può rendere necessaria la consegna di ulteriori informative laddove sia fondamentale fornire all'interessato ulteriori informazioni (ad esempio l'informativa SIC).

Nel caso di servizi commercializzati da soggetti terzi per conto della società Titolare del trattamento, questa, mediante apposita previsione inserita nella convenzione, può incaricare il soggetto terzo alla consegna dell'informativa allorché quest'ultimo abbia il contatto diretto con l'interessato.

Contestualmente alla consegna dell'informativa, laddove necessario, vengono raccolti anche i consensi per poter svolgere i trattamenti per i quali è necessario il consenso dell'interessato (es. marketing).

Per le modalità con le quali vengono raccolti i consensi si rimanda ai paragrafi successivi.

A seguito dell'evoluzione normativa o aziendale, è possibile che l'informativa alla clientela subisca delle variazioni. In questo caso, il modello aggiornato di informativa è reso sempre disponibile sul sito internet della singola banca o società.

6.5 INFORMATIVA SITO WEB E COOKIES

La Banca/Società del gruppo in possesso di un sito web è tenuta a pubblicare un'apposita informativa che rispetti tutti i requisiti richiesti dall'art. 13 del GDPR. Dovrà, in particolare, contenere la descrizione delle tipologie di dati personali raccolti tramite la piattaforma: i dati di navigazione (quali ad esempio gli indirizzi IP, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, ecc…), i dati forniti volontariamente dall'utente, ecc… oltre che tutti gli altri elementi, quali la base giuridica che giustifica il trattamento, le finalità (quali ad esempio quelle relative alla raccolta di dati personali per le attività di marketing, trasmissione di newsletter o messaggi istantanei, ecc.) e tutti gli altri elementi richiesti dalla normativa.

Tale informativa viene definita come "informativa estesa" e deve essere facilmente reperibile dall'utente che sta navigando sul sito della Banca (ad esempio tramite un apposito link all'interno del footer del sito che rimanda all'informativa).

Si evidenzia inoltre che è buona prassi inserire, all'interno delle pagine dedicate alla raccolta dei dati personali, prima del tasto "submit" del form, l'indicazione della finalità per la quale l'utente intende trasmettere i dati personali unitamente al link che riporta alla pagina in cui è pubblicata l'informativa privacy estesa.

Oltre la pubblicazione dell'informativa destinata alle elaborazioni collegate al sito web è necessario pubblicare l'informativa estesa che descrive i cookies impiegati dal sito. I cookie sono piccoli file di testo che i siti visitati inviano al terminale (computer, tablet, smartphone, notebook) dell'utente, dove vengono memorizzati, per poi essere ritrasmessi agli stessi siti alla visita successiva. Sono usati per eseguire autenticazioni informatiche, monitoraggio di sessioni e memorizzazione di informazioni sui siti. A titolo esemplificativo, l'accesso all'home banking e le attività che possono essere svolte sul proprio conto corrente online (visualizzazione dell'estratto conto, bonifici, pagamento di bollette, ecc.) sarebbero molto più complesse da svolgere e meno sicure senza la presenza di cookie che consentono di identificare l'utente e mantenerne l'identificazione nell'ambito della sessione.

Va precisato, inoltre, che attraverso i cookie è possibile monitorare la navigazione, raccogliere dati su gusti, abitudini, scelte personali che, di fatto, consentono la ricostruzione dettagliata dei profili dei consumatori (c.d. profilazione).

Il Garante ha operato una distinzione tra cookie "tecnici" e "di profilazione", dalla quale consegue l'ambito di operatività per il quale è necessario ottenere dall'utente il consenso al trattamento, rispetto all'ambito per il quale non è necessario acquisire il consenso. Nella tabella sottostante sono sintetizzate le misure necessarie che il titolare/ gestore del sito deve adottare per adeguarsi alla normativa Privacy.

Tipologie	**Descrizione di dettaglio**	**Misure necessarie**
Cookie tecnici	• i cookie di navigazione o di sessione, relativi ad attività strettamente necessarie al funzionamento e all'erogazione del servizio (sono quelli che permettono di realizzare un acquisto o l'autenticazione per l'accesso alle aree riservate); • i cookie di funzionalità, relativi ad attività di salvataggio delle preferenze e ottimizzazione (ad esempio, cookie flash player se non superano la durata della sessione, cookie di salvataggio del carrello o delle preferenze sulla lingua/valuta; • cookie analytics laddove utilizzati direttamente dal gestore del sito per raccogliere informazioni, in forma aggregata, sul numero degli utenti e su come visitano il sito.	Deve essere sempre e comunque disponibile un'**informativa estesa** (ai sensi dell'art. 13 del Codice) che fornisca informazioni circa l'utilizzo e le finalità dei cookie presenti sul sito. **Non è necessario** fornire all'utente l'informativa breve. **Non è necessario il consenso dell'utente.**
Cookie non tecnici	• cookie di statistica gestiti completamente dalle terze parti se non sono adottati strumenti di terze parti che riducono il potere identificativo • cookie di profilazione pubblicitaria di prima o terza parte; • cookie di social network;…	Occorre mostrare su qualsiasi pagina di primo accesso al sito **l'informativa breve tramite un banner dinamico** che dovrà costituire una percettibile discontinuità nella fruizione dei contenuti. **È necessario inoltre il consenso dell'utente**.

Come si evince dalla tabella sopra riportata, **tutti i cookie qualificabili come "non tecnici"**, che, peraltro, presentano maggiori criticità con riguardo alla tutela della sfera personale degli utenti, come ad esempio, quelli usati per finalità di profilazione e marketing, **non possono essere installati sui terminali degli utenti stessi se questi non siano stati prima adeguatamente informati e non abbiano prestato al riguardo un valido consenso.**

Cookie non tecnici: Informativa breve

Nel momento in cui l'utente accede alla home page dovrà comparire un banner contenente un'informativa breve e un conseguente consenso. Questo dovrà essere collocato in modo da risultare ben visibile e recare un chiaro avviso che l'installazione del sito potrà comportare l'installazione di cookies o la raccolta di dati dell'utente per finalità di pubblicità comportamentale. Il superamento della presenza del banner al video deve essere possibile solo mediante un intervento attivo dell'utente (appunto attraverso la selezione di un elemento contenuto nella pagina sottostante il banner stesso).

L'**informativa breve** dovrà contenere le seguenti indicazioni:

a) che il sito utilizza cookie di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete;
b) che il sito consente anche l'invio di cookie a "terze parti" (laddove ciò ovviamente accada);
c) il link all'informativa estesa;
d) l'indicazione delle modalità con le quali è possibile negare il consenso all'installazione di qualunque cookie;

Cookie di terze parti.

La normativa distingue altresì tra *cookie del gestore del sito*, definito come "editore", e *cookie di "terze parti"* ovvero cookie gestiti completamente dalle terze parti (ad. esempio cookies analytics), al fine di individuarne i rispettivi ruoli e responsabilità. In quest'ultimo caso, gli editori devono essere considerati, da un lato, titolari del trattamento dei cookie installati direttamente e, dall'altro, quali intermediari tecnici tra le terze parti e gli utenti[1].

Nel caso in cui un sito consenta la trasmissione anche di cookie di "terze parti", l'informativa e l'acquisizione del consenso sono di norma a carico del terzo.

È quindi sufficiente che l'utente venga reindirizzato all'informativa della terza parte.

[1] Garante per la protezione dei dati personali: Provvedimento dell'8 maggio 2014 Faq in materia di cookie

L'informativa cookie estesa.

L'informativa cookie estesa contiene tutti gli elementi previsti dall'art. 13 del GDPR e descrive le caratteristiche e le finalità dei cookies installati dal sito.

Deve essere raggiungibile mediante un link inserito nell'informativa breve, come pure attraverso un riferimento su ogni pagina del sito, collocato in calce alla medesima.

All'interno di tale informativa, deve essere inserito anche il link aggiornato alle informative e ai moduli di consenso delle terze parti con le quali l'editore ha stipulato accordi per l'installazione di cookies tramite il proprio sito. Qualora l'editore abbia contatti indiretti con le terze parti, dovrà linkare i siti dei soggetti che fanno da intermediari tra lui e le stesse terze parti.

Al fine di mantenere distinta la responsabilità degli editori da quella delle terze parti in relazione all'informativa resa e al consenso acquisito per i cookie di queste ultime tramite il proprio sito, il Garante ha previsto che, in sede contrattuale, gli editori stessi acquisiscano i suindicati link dalle terze parti.

Nel medesimo spazio dell'informativa estesa deve essere richiamata la possibilità per l'utente (alla quale fa riferimento anche l'art. 122, comma 2, del Codice) di manifestare le proprie opzioni in merito all'uso dei cookie da parte del sito anche attraverso le impostazioni del browser, indicando almeno la procedura da eseguire per configurare tali impostazioni.

L'informativa estesa deve necessariamente contenere:

- una spiegazione generale di che cosa sono i cookie e della gestione degli stessi tramite le impostazioni dei browser;
- la spiegazione di come viene prestato il consenso;
- la descrizione delle categorie di cookie tecnici suddivisi per finalità;
- la descrizione di cookie del Titolare o del gestore del sito con il relativo "modulo" (box, spunta o altro) per il consenso;
- la descrizione delle finalità dei cookie di terze parti ed il relativo link alla informativa e consenso della terza parte con la quale il gestore del sito ha stipulato accordi per l'installazione dei cookie sul proprio sito, ove disponibili; oppure il link al sito degli intermediari (solitamente il concessionario di pubblicità del sito) ove presenti.

6.6 INFORMATIVA RELATIVA AD UN SISTEMA DI INFORMAZIONI CREDITIZIE GESTITO DA SOGGETTI PRIVATI

In aggiunta all'informativa clientela, qualora la Banca o la Società del Gruppo partecipi ad un sistema di informazioni creditizie **gestito da soggetti privati**, il dipendente, al momento della raccolta dei dati personali relativi a richieste/rapporti di credito, informa l'Interessato anche con riguardo al trattamento dei dati personali effettuato nell'ambito del sistema di informazione creditizia e fornisce apposita informativa.

A seguito dell'evoluzione normativa o aziendale, è possibile che l'informativa per l'impiego dei SIC subisca delle variazioni. In questo caso, il modello aggiornato di informativa è reso sempre disponibile sul sito internet della singola banca o società del Gruppo.

6.7 INFORMATIVA IN CASO DI CESSIONE IN BLOCCO E CARTOLARIZZAZIONE DEI CREDITI

Nei casi previsti, i cessionari di crediti in blocco possono fornire l'informativa in forma non individualizzata, a condizione che le informazioni siano rese comunque conoscibili, in modo tale da consentire l'individuazione univoca, secondo parametri obiettivi e predeterminati, delle posizioni debitorie oggetto di cessione, mediante l'adozione delle seguenti misure:

a) pubblicazione nella Gazzetta Ufficiale della Repubblica italiana dell'informativa;
b) successiva comunicazione ai debitori ceduti alla prima occasione utile.

6.8 INFORMATIVA IN CASO DI FUSIONE

Con riferimento alle operazioni di fusione e scissione fra società, si precisa che le società coinvolte in operazioni di scissione e fusione devono fornire agli interessati i necessari aggiornamenti rispetto all´informativa resa dalla società scissa e dalle società partecipanti alla fusione e, tra essi, in particolare, la nuova denominazione del titolare del trattamento e gli estremi identificativi dell´eventuale nuovo responsabile presso il quale esercitare il diritto di accesso ai dati personali, secondo le seguenti modalità:

a) attraverso il sito web delle società interessate dalle operazioni di scissione e fusione, in corrispondenza del loro verificarsi;
b) con comunicazione individualizzata agli interessati in occasione della prima circostanza utile di contatto, anche per altre finalità.

Inoltre, non è necessario raccogliere nuovamente i consensi nella misura in cui essi abbiano le stesse caratteristiche di quelli precedentemente raccolti.

6.9 INFORMATIVA PRODOTTI DI TERZI[2]

Laddove un cliente manifesti l'intenzione di voler accendere un rapporto con terzi per il tramite della Banca, la quale agisce quale collocatore di prodotti altrui, è necessario che:

- l'operatore bancario avverta oralmente il cliente che i dati impiegati per l'accensione del nuovo rapporto sono quelli presenti nell'anagrafica della Banca, fatta salva la possibilità per l'interessato di opporsi e conferire dati diversi;
- l'operatore inviti il cliente a verificare, prima della sottoscrizione del contratto con la società terza, la correttezza dei dati ivi inseriti;
- laddove concordato con la società terza, l'operatore fornisca al cliente l'informativa sul trattamento di dati personali della società.

6.10 CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Dopo aver fornito l'informativa di cui alle sezioni precedenti, il dipendente o i soggetti terzi a ciò delegati mediante apposita convenzione raccolgono il/i consenso/i espresso dell'Interessato al trattamento dei dati personali, laddove previsto.

Il/i consenso/i è/sono raccolto/i con specifica sottoscrizione dell'Interessato sui moduli prodotti dalle procedure in uso o predisposti dal Servizio DPO a seconda della tipologia di rapporto instaurato.

Il Titolare del trattamento deve essere sempre in grado di dimostrare che l'interessato ha prestato il consenso, non è mai ammesso il consenso tacito o presunto e neppure le caselle pre - spuntate.

Ogni consenso è valido se è stato espresso dall'interessato liberamente, in modo inequivocabile e specificamente con riguardo a ciascuna finalità e può essere revocato in ogni momento.

6.11 RACCOLTA CONSENSO CLIENTELA ALLO SPORTELLO[3]

Per quanto attiene specificatamente al consenso raccolto dal cliente che si reca presso lo sportello, al fine di evitare problemi di difformità tra quanto optato dal cliente e quanto inserito nella procedura telematica dal singolo operatore, è stata elaborata una procedura che permette di eliminare il margine di errore in capo all'addetto.

---

[2] Capitolo applicabile solo agli intermediari finanziari.
[3] Capitolo applicabile solo alle Banche.

La procedura prevede quanto segue:

1) l'addetto consegna l'informativa e il modulo di raccolta di consenso al cliente;
2) l'addetto legge insieme al cliente le possibili scelte;
3) il cliente manifesta il proprio consenso oralmente;
4) l'addetto inserisce contemporaneamente le scelte del cliente nella procedura informatica;
5) l'addetto stampa e consegna al cliente il modulo di consenso con le caselle spuntate, come da scelte espresse dal cliente;
6) il cliente verifica il contenuto del modulo e lo sottoscrive.

Tale procedura è adottata per tutti i clienti che si recano fisicamente presso una filiale della Banca.

Le modalità sopra descritte possono essere integrate e modificate sulla base dell'evoluzione tecnologica a cui la Banca è sottoposta.

In alternativa, a titolo esemplificativo, è possibile l'impiego di tablet, smartphone e sistemi di ultima generazione per la raccolta del consenso, purché garantiscano all'interessato di esprimere il proprio consenso in modo libero ed inequivocabile attraverso un'azione positiva, in accordo con quanto previsto dalla vigente normativa. Nel caso di rifiuto dell'Interessato alla concessione del consenso necessario per lo svolgimento di un determinato trattamento (se il consenso risulta essere l'unica valida base giuridica per il trattamento), lo stesso non potrà essere eseguito.

Il dipendente o i soggetti terzi a ciò delegati mediante apposita convenzione provvedono all'archiviazione dei documenti attestanti il/i consenso/i dell'Interessato unitamente alla documentazione relativa al rapporto contrattuale instaurato con lo stesso.

6.12 RACCOLTA CONSENSO DAL SITO WEB

Laddove la base giuridica per la raccolta di dati personali mediante le pagine del sito web sia il consenso, sono necessarie, ai sensi dei principi stabiliti dal GDPR, specifiche implementazioni informatiche capaci di dimostrare la raccolta del consenso per ogni specifica finalità da parte di ogni utente in una determinata data.

Le medesime implementazioni informatiche sono necessarie per la raccolta dei consensi relativi i a cookies impiegati per finalità di marketing / remarketing.

Il Titolare del sito deve progettare i meccanismi per l'acquisizione del consenso evitando ambiguità e garantendo che l'azione con la quale viene prestato il consenso possa essere distinta da altre azioni. Pertanto, la mera continuazione dell'uso ordinario di un sito web non è una condotta da cui

si può dedurre un'indicazione della volontà dell'interessato di manifestare il proprio consenso all'esecuzione di un'elaborazione. In base al considerando 32 del GDPR, inoltre, azioni come lo scorrimento di una pagina web o altre assimilabili, non possono essere considerate come azioni chiare ed affermative. In tal caso, inoltre, sarebbe difficile fornire all'utente un modo per revocare il consenso con la stessa facilità con cui l'ha concesso.

Il Titolare dovrà conservare, con modalità informatiche, l'espressione di consenso per i cookies di profilazione nel rispetto dei principi del GDPR.

7. Trattamento nell'ambito dei Sistemi Informativi Creditizi (SIC)[4]

La Banca, in quanto Titolare del trattamento di dati personali raccolti in relazione a richieste/rapporti di credito, può partecipare – in virtù di apposito contratto o accordo con il gestore – ad un sistema di informazioni creditizie gestito da una persona giuridica, un ente, un'associazione o un altro organismo in ambito privato.

L'impiego dei sistemi informativi creditizi gestiti da soggetti privati è regolato dal relativo Codice di condotta approvato dall'Autorità Garante per la protezione dei dati personali con Provvedimento n. 163 del 12 settembre 2019.

Al fine di meglio valutare il rischio di credito, nonché l'affidabilità e puntualità nei pagamenti degli interessati la Banca, in qualità di "partecipante", comunica alcuni dati (dati anagrafici, anche della persona eventualmente coobbligata, tipologia del contratto, importo del credito, modalità di rimborso) ai sistemi di Sistema di Informazioni Creditizie, i quali, nella qualità di autonomo titolare del trattamento, valutano l'affidabilità e puntualità nei pagamenti degli interessati.

L'accesso, la conservazione e la trasmissione dei dati personali vengono effettuati sulla base giuridica del legittimo interesse del titolare del trattamento a consultare i SIC. Non è, quindi, necessaria l'espressione del consenso dell'interessato per l'accesso ai SIC o per le contribuzioni periodiche dei dati. La banca potrà accedere/comunicare i dati al SIC previa consegna dell'informativa specifica all'interessato; la stessa informativa SIC dovrà, inoltre, essere pubblicata sul sito internet della banca.

Il trattamento dei dati personali contenuti in un sistema di informazioni creditizie è effettuato dal gestore e dai partecipanti esclusivamente per finalità correlate alla tutela del credito e al

[4] Capitolo applicabile solo alle Banche.

contenimento dei relativi rischi e, in particolare, per valutare la situazione finanziaria e il merito creditizio degli Interessati o, comunque, la loro affidabilità e puntualità nei pagamenti. Non può essere perseguito alcun altro scopo non previsto dal Codice di Condotta, specie se relativo a ricerche di mercato, pubblicità e promozione o vendita diretta di prodotti o servizi.

I dati personali degli interessati sono oggetto di particolari elaborazioni statistiche al fine di attribuire un giudizio sintetico o un punteggio sul grado di affidabilità e solvibilità (c.d. credit scoring), tenendo conto delle seguenti principali tipologie di fattori: numero e caratteristiche dei rapporti di credito in essere, andamento e storia dei pagamenti dei rapporti in essere o estinti, eventuale presenza e caratteristiche delle nuove richieste di credito, storia dei rapporti di credito estinti.

Al verificarsi di ritardi nei pagamenti, la banca partecipante, anche unitamente all'invio di solleciti o di altre comunicazioni, o eventualmente con le modalità indicate nel contratto, deve inviare all'interessato un preavviso circa l'imminente registrazione dei dati in uno o più SIC (segnalazioni negative). I dati relativi al primo ritardo possono essere resi accessibili ai partecipanti solo decorsi almeno quindici giorni dalla spedizione del preavviso all'interessato.

8. Videosorveglianza

L'esercizio dell'attività bancaria-assicurativa e più in generale delle attività ad essa connesse implica la presenza materiale di denaro contante, valori ed altri beni strumentali presso la sede della Banca/Società del Gruppo. I luoghi in cui si trovano tali beni rappresentano da sempre un concreto obiettivo di furti, rapine, danneggiamenti, atti di vandalismo, esponendo sia il personale dipendente che la clientela a situazioni di pericolo, anche per la loro incolumità fisica.

Nel bilanciamento degli interessi risulta prevalente la necessità di garantire un adeguato livello di sicurezza a dipendenti e clienti e di protezione del patrimonio aziendale, rispetto ai diritti e alle libertà dell'interessato.

Le immagini sono raccolte ed utilizzate esclusivamente per le finalità sopra descritte attraverso l'adozione di adeguate misure di sicurezza e l'individuazione di personale espressamente incaricato alla consultazione delle immagini.

Il trattamento dei dati relativi alla videosorveglianza avviene in conformità della normativa sulla protezione dei dati con particolare riferimento al Provvedimento del Garante Privacy dell'8 aprile 2010 e successive modifiche e alle Linee guida 3/2019 dell'EDPB.

Nell'esecuzione del trattamento, il Titolare si attiene al principio di necessità e minimizzazione, il quale comporta un obbligo di attenta configurazione dei sistemi informativi e dei programmi informatici per ridurre al minimo l'utilizzazione di dati personali, e al principio di proporzionalità nella

scelta delle modalità di ripresa e dislocazione nonché nelle varie fasi del trattamento, che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite.

Nell'uso delle apparecchiature volte a riprendere aree esterne ad edifici e immobili (perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza), la Banca/Società del Gruppo garantisce che il trattamento sia effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti e di particolari che non risultino rilevanti (vie, edifici, esercizi commerciali, istituzioni ecc.), oltre a vietare qualsiasi forma di controllo a distanza dell'attività lavorativa.

Per quanto attiene al profilo della sicurezza dei dati oggetto di trattamento tramite apparecchiature di videosorveglianza, la Banca/Società del Gruppo:

- adotta impostazioni predefinite che riducano al minimo il trattamento dei dati non solo a livello di progettazione della tecnologia, ma anche nelle pratiche organizzative;
- predispone un adeguato sistema di verifica e di gestione degli accessi ai sistemi di dati videoregistrati, definendo i livelli di visibilità e trattamento delle immagini;
- fornisce le necessarie istruzioni operative agli autorizzati al trattamento;
- adotta idonee e preventive misure di sicurezza atte a ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato, anche accidentale, o trattamento non consentito o non conforme alle finalità della raccolta dei dati acquisiti mediante apparecchiature di videosorveglianza;
- predispone un sistema digitale programmato in modo tale da operare, al momento prefissato, alla cancellazione automatica dei dati da ogni supporto, fatti salvi i casi eccezionali in cui le immagini possono esser conservate per necessità debitamente documentate, tra le quali quelle di consegnarne una copia dall'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.

9. Misure di Sicurezza e Attività non consentite

9.1. SICUREZZA DELLA DOCUMENTAZIONE CARTACEA

I locali e tutti i supporti fisici utilizzati nei diversi ambienti di lavoro, compresa la documentazione cartacea della Banca/Società del Gruppo, devono essere protetti con la massima diligenza e nel

rispetto delle procedure di lavoro definite, al fine di prevenire danni conseguenti ad azioni di carattere doloso/colposo.

In particolare, tutti i dipendenti e collaboratori sono tenuti al rispetto delle seguenti regole generali:

- i visitatori accedono alle sedi e filiali sempre accompagnati dal personale dipendente, nei casi in cui è previsto, previa registrazione su appositi registri presenti presso la reception;
- i visitatori possono accedere alle sole aree coerenti rispetto alle ragioni della loro visita e, ove previsto, al termine della visita è necessario verificare la corretta registrazione dell'uscita;
- sono autorizzati ad accedere ai dati trattati in una specifica area o ufficio, i soli utenti che vi prestano servizio o che hanno pertinenza con il tipo di attività svolta;
- i documenti contenenti dati personali devono essere utilizzati e conservati con la massima cura all'interno di aree o uffici ad accesso controllato;
- al termine della giornata lavorativa i documenti contenenti dati personali dovranno essere riposti e conservati all'interno uffici chiusi a chiave o, perlomeno, di armadi chiusi a chiave;
- la documentazione non più necessaria deve essere eliminata attraverso le previste procedure e i documenti contenenti dati personali devono essere distrutti attraverso strumenti che ne impediscano la ricostruzione;
- è vietato lasciare incustoditi fax, fotocopie, stampe presso le apposite apparecchiature;
- in caso di stampe multiple, va prestata particolare attenzione alla verifica della coda di stampa, al fine di accertare che nessuno dei documenti mandati in stampa sia rimasto in sospeso;
- i documenti contenenti dati personali, se portati al di fuori delle sedi aziendali, devono essere custoditi con la massima cura e non devono essere lasciati incustoditi in luoghi pubblici.

I documenti cartacei devono essere:

- conservati in archivi adeguatamente protetti, per evitare la lettura e/o il prelievo non autorizzato dei documenti cartacei, garantendo, quindi, la riservatezza e l'integrità dei dati personali e/o "categorie particolari di dati personali", in essi contenuti;
- riposti negli appositi archivi che, al termine della giornata lavorativa, dovranno essere chiusi a chiave in armadi o stanze. Le chiavi dovranno essere risposte in un luogo sicuro e non lasciate nelle serrature stesse;

- trasferiti presso gli archivi centrali quando non più operativamente necessari.