Regole aziendali per il trattamento e la protezione dei dati personali delle Persone Fisiche

Normativa attinente ad aree sensibili relative al D.Lgs. 231/01

Area di rischio: Reati contro la Pubblica Amministrazione
Protocolli: Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la
Pubblica Amministrazione
Gestione dei rapporti con le Autorità di Vigilanza

Area di rischio: Reati informatici
Protocolli: Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo

Emittente:
Direzione Centrale Tutela Aziendale

Destinatari:
Intesa Sanpaolo

Percorso:
ARCO – Regole – Gestione Rischi e Controlli – Gestione della Conformità

Decorrenza: Giugno 2020

INTESA SANPAOLO

INDICE

Premessa

Le presenti *Regole aziendali per il trattamento e la protezione dei dati personali delle Persone Fisiche* (di seguito le 'Regole') sono emanate al fine di fornire un quadro delle norme e dei comportamenti relativi al trattamento e alla protezione dei dati personali e si rivolgono a tutti i lavoratori dipendenti, nonché ai collaboratori della Banca.

Le Regole dettagliano gli argomenti pertinenti alle attività ed ai trattamenti svolti dalla Banca e contengono specifiche disposizioni operative al fine di ottemperare alle previsioni del Regolamento (UE) 2016/679[1] (di seguito 'General Data Protection Regulation' o 'GDPR' o 'Regolamento') del Parlamento Europeo e del Consiglio, che disciplina la protezione dei dati personali delle persone fisiche, nonché la libera circolazione di tali dati nell'Unione Europea, e di tutta la normativa nazionale ed europea[2] vigente connessa alla materia.

La normativa europea e nazionale in materia di protezione dei dati personali responsabilizza ciascun Titolare del trattamento all'attuazione degli opportuni interventi regolamentari, organizzativi e tecnologici, al fine di rispondere adeguatamente ai requisiti prescritti secondo un approccio *risk based* (c.d. "principio di *accountability*").
Qualsiasi trattamento di dati personali effettuato da un Titolare o Responsabile del trattamento stabilito nel territorio dell'Unione Europea deve essere conforme ai requisiti disposti dal Regolamento, indipendentemente dal fatto che il trattamento avvenga all'interno dell'Unione. La normativa si applica anche ai trattamenti svolti da Titolari o Responsabili non stabiliti nell'Unione quando le attività di trattamento riguardano dati personali degli interessati che si trovano nell'Unione[3].
In via preliminare, si raccomanda la consultazione delle Definizioni disposte nel presente documento a riferimento sulla terminologia specifica in uso sulla materia ed entro le Regole.

([1]) Tale Regolamento, efficace dal 25 maggio 2018, abroga la precedente Direttiva 95/46/CE ed è direttamente applicabile in tutti gli Stati membri.

([2]) Le Filiali della Banca ubicate in Paesi diversi dall'Italia ma nel perimetro UE applicano le presenti Regole previa verifica della loro compatibilità con la normativa locale di attuazione del GDPR, che deve essere sottoposta preventivamente all'esame della struttura emittente.

([3]) Quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

1 LE PRINCIPALI FONTI NORMATIVE

1.1 Regolamento UE 2016/679

Come indicato, il principale riferimento normativo in materia di protezione dei dati personali è costituito dal Regolamento (UE) 2016/679, che prevede tra l'altro:

- l'applicazione dei principi di Privacy by Design e Privacy by Default per garantire il presidio del rischio di non conformità alla normativa sul trattamento e protezione dei dati personali sia nelle fasi di ideazione o di modifica sostanziale di trattamento di dati personali, sia durante il trattamento, mediante l'adozione, come impostazione predefinita, delle opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato;
- la redazione e l'aggiornamento, nel continuo, del Registro delle attività di trattamento;
- lo svolgimento di un *Privacy Impact Assessment* (c.d. "P.I.A.") prima di procedere a uno o più trattamenti che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- la nomina del Responsabile della Protezione dei dati - Data Protection Officer (di seguito anche 'DPO');
- l'individuazione e l'istruzione delle persone autorizzate al trattamento;
- la nomina e l'istruzione del Responsabile (esterno) del trattamento, laddove necessario;
- l'identificazione di eventuali Contitolari del trattamento e la formalizzazione dei relativi accordi;
- la definizione e manutenzione di un catalogo di controlli in materia Privacy;
- la notifica delle violazioni di dati personali (o c.d. "*Data Breach*") all'Autorità di Controllo e la relativa eventuale comunicazione agli interessati;
- l'attuazione delle misure atte a garantire l'effettivo esercizio, da parte degli interessati, dei diritti riconosciuti dal Regolamento;
- l'erogazione di iniziative di formazione e diffusione di cultura della Privacy.

1.2 Codice Privacy (D.Lgs. 196/2003 modificato dal D.Lgs. 101/2018)

A livello nazionale vige il Decreto Legislativo n. 196 del 30 giugno 2003 (c.d. "Codice Privacy") previgente al GDPR, come modificato dal Decreto Legislativo n. 101 del 10 agosto 2018, che adegua la normativa nazionale al GDPR, introducendo e specificando aspetti fondamentali concernenti la protezione dei dati personali e, al contempo, integrando e ordinando le disposizioni già in vigore.

1.3 Linee Guida e Provvedimenti del Garante Privacy

Le Linee Guida e i Provvedimenti del Garante per la protezione dei dati personali, sulla base delle indicazioni fornite da tale Autorità, continuano a essere applicabili anche a seguito dell'entrata in vigore del GDPR, in quanto compatibili con tale regolamento e con le disposizioni del d.lgs. 101/2018.

Per una prima consultazione si segnalano in particolare i provvedimenti in Appendice al presente documento.

1.4 Documenti dell'European Data Protection Board

Ai fini dell'applicazione del GDPR rilevano, inoltre, i documenti dell'European Data Protection Board (anche "EDPB") o Comitato europeo per la protezione dei dati (che ha sostituito il Working Party 29 o 'WP29'), quale organo europeo indipendente, previsto dall'art. 70 del GDPR, composto dai rappresentanti delle Autorità nazionali di controllo in materia di protezione dei dati personali degli Stati dell'Unione Europea e dal Garante europeo per la protezione dei dati. È compito dell'EDPB garantire l'applicazione coerente del Regolamento.
Per una prima valutazione della documentazione di rilievo si veda quanto riportato in Appendice al presente documento.

2 DEFINIZIONI

Di seguito si riportano alcune definizioni fondamentali riferite al Regolamento e alla normativa in materia in relazione all'applicazione organizzativa in azienda.

- **«amministratore di sistema»**[4]**:** figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché, anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning), le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
- **«archivio»/«banca dati»**: qualsiasi insieme strutturato contenente dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **«Autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR **(**per l'Italia il Garante per la Protezione dei Dati Personali);
- **«Autorizzato»**: la persona fisica autorizzata e istruita a compiere operazioni di trattamento dei dati personali dal Titolare o dal Responsabile;
- **«consenso dell'Interessato»**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva esplicita, che i dati personali che lo riguardano siano oggetto di trattamento;
- **«Contitolari del trattamento»**: figura prevista dall'articolo 26 del GDPR allorché due o più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento realizzato in varie operazioni o insiemi di operazioni su dati personali, che possono avere luogo simultaneamente o in varie fasi;
- **«criterio minimo privilegio»:** principio secondo cui la visibilità delle informazioni è limitata alle sole informazioni immediatamente necessarie alla funzione.
- **«cookie»**: stringhe di testo che i siti web visitati rilasciano sul dispositivo elettronico impiegato nella visita/navigazione, permettendo il riconoscimento dello stesso alla successiva visita. Sono usati per eseguire autenticazioni automatiche, monitoraggio di sessioni e memorizzazioni di

[4] L'Autorità Garante non ha inteso equiparare gli "operatori di sistema" di cui agli articoli del Codice penale relativi ai delitti informatici, con gli "Amministratori di Sistema", questi ultimi sono dei particolari operatori di sistema, dotati di specifici privilegi. Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.

informazioni riguardanti gli utenti che accedono al server (rispettivamente c.d. cookie tecnici, cookie analytics, cookie di profilazione);

- **«Data Protection Officer – DPO»**: il Responsabile della protezione dei dati istituito ai sensi del Regolamento europeo;
- **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **«dati relativi alla salute»**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **«dato anonimo»**: il dato che, in origine o a seguito di un processo di anonimizzazione irreversibile, non può consentire l'identificazione di un Interessato;
- **«dato giudiziario»**: il dato personale idoneo a rivelare provvedimenti in materia di casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione), 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; **«dato identificativo»**: il dato personale che permette l'identificazione diretta dell'Interessato;
- **«dato particolare»**: dati personali che rivelano 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;
- **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
- **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi[5];

[5] Tuttavia, le Autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il

- **«Garante per la Protezione dei Dati Personali»**: l'Autorità preposta alla vigilanza del rispetto della normativa sulla protezione dei dati personali in Italia. Organo collegiale costituito da quattro componenti, due eletti dalla Camera dei Deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni. L'attività del Garante copre ogni settore della vita sociale, economica e culturale del Paese in cui si manifesti l'esigenza della protezione dei dati personali;
- **«Interessato»**: la persona fisica cui si riferiscono i dati personali[6];
- **«misure di sicurezza»**: l'insieme delle misure tecniche, informatiche, organizzative, logistiche e procedurali volte a mitigare i rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o trattati;
- **«data protection by design and by default»**: principi contenuti nel GDPR volti a garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e ad adottare comportamenti che consentano di prevenire possibili problematiche nonché a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Si veda l'articolo 25 del GDPR;
- **«privacy impact assessment»** procedura prevista dall'articolo 35 del GDPR (prescritta in particolare per i casi in cui il trattamento dei dati può presentare un rischio elevato per i diritti e le libertà delle persone fisiche) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli;
- **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo dei medesimi per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **«profili di autorizzazione»**: l'insieme delle informazioni, univocamente associate ad un Autorizzato, che consente di individuare a quali dati possa accedere, nonché i trattamenti ad esso consentiti;
- **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un Interessato specifico senza l'utilizzo di informazioni aggiuntive, a

---

trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

(6) Nell'ordinamento italiano sono giuridicamente equiparate alla persona fisica le ditte individuali ed i liberi professionisti (cfr. anche *Provvedimento del Garante n.217 del 24 aprile 2013*).

condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative tese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- **«Registro delle attività di Trattamento»**: documento contenente le principali informazioni (specificatamente individuate dall'articolo 30 del GDPR) relative alle operazioni di trattamento svolte dal Titolare e, se nominato, dal Responsabile del trattamento;
- **«Registro pubblico delle opposizioni»**: registro al quale è possibile, per qualunque abbonato telefonico, iscriversi con modalità semplificate e anche in via telematica, al fine di opporsi all'utilizzo per finalità pubblicitarie dei numeri di telefono di cui si è intestatari e dei corrispondenti indirizzi postali associati, presenti negli elenchi pubblici, da parte degli operatori che svolgono attività di marketing tramite il telefono e/o la posta cartacea[7];
- **«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;
- **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
- **«Titolare del trattamento»**: 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 del 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, la visualizzazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **«violazione dei dati personali»/«data breach»**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica/ compromissione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

[7] Il Regolamento di estensione del Registro Pubblico delle Opposizioni alle numerazioni fisse e mobili non riportate negli elenchi telefonici pubblici, è in fase di approvazione secondo quanto stabilito dalla Legge n.5/2018.

3 LE PRINCIPALI PREVISIONI NORMATIVE

Da un punto di vista generale e confermando i principi già contenuti nella precedente Direttiva 95/46/CE, il GDPR ribadisce che per trattamento di dati personali si intende: "*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*".

Oggetto di protezione sono i dati personali delle "persone fisiche" (ivi compresi liberi professionisti e imprese individuali) con esclusione di ogni altra figura (ad esempio, società di persone e di capitali, società cooperative, associazioni, fondazioni, consorzi e altri enti di carattere pubblico e privato). Il GDPR definisce la persona fisica cui i dati personali si riferiscono con l'espressione di "**Interessato**".

Per quanto riguarda il trattamento dei dati delle persone giuridiche, enti o associazioni permangono le tutele fissate dall'art. 130 del Codice Privacy ("Comunicazioni indesiderate") e in particolare la necessità di acquisire il consenso per lo svolgimento di attività promozionali o il compimento di ricerche di mercato effettuati sia con sistemi automatici di comunicazione sia con comunicazioni elettroniche (posta elettronica, telefax, SMS, MMS, ecc. …)[8].

3.1 Modalità e finalità del trattamento dati

In ottemperanza alle previsioni normative i dati devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato ("liceità, correttezza e trasparenza");
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità ("limitazione delle finalità");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");

[8] Cfr. *Provvedimento del Garante del 20 settembre 2012* in ordine all'applicabilità alle persone giuridiche del codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.lgs. n. 201/2011.

- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento a tutela dei diritti e delle libertà dell'Interessato ("limitazione della conservazione");

- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

Il Titolare del trattamento è competente per il rispetto di quanto sopra esposto e deve essere in grado di comprovarlo ("responsabilizzazione").

Il Regolamento prevede che le modalità di trattamento dei dati personali devono essere impostate sin dall'inizio in modo da escluderne l'utilizzo quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi, ovvero seguendo opportune modalità che permettano di identificare l'Interessato solo in caso di necessità.

3.2 Informativa e principio di liceità del trattamento

Il GDPR individua nella trasparenza verso gli Interessati uno degli elementi cardine della disciplina, pertanto dispone analiticamente i contenuti e le regole di predisposizione dell'informativa agli Interessati (artt. 13 e 14 del Regolamento).

L'Informativa deve essere resa all'Interessato, o "*alla persona presso la quale sono raccolti i dati personali*", prima della raccolta degli stessi e prima di qualunque trattamento le cui finalità si discostino da quelle dichiarate al momento della raccolta dei dati.

Nel caso in cui i dati non siano raccolti presso l'Interessato, l'Informativa (art. 14) deve essere fornita allo stesso entro un termine ragionevole e comunque entro un mese dall'ottenimento dei dati personali. Tuttavia, ove si preveda la comunicazione dei dati personali all'Interessato o la rivelazione di essi a terzi, è permesso procedere alla resa dell'Informativa al più tardi al momento rispettivamente della prima comunicazione o della prima rivelazione.

In tale ultimo caso, il Regolamento prevede l'esonero dall'obbligo di rendere l'Informativa qualora: i) l'Interessato disponga già delle informazioni, ii) comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato, iii) l'ottenimento o la comunicazione siano espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento iv) i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri.

Al fine di stabilire la liceità del trattamento, la Funzione di business e di supporto, avvalendosi della consulenza del Data Protection Officer e, ove necessario, della Direzione Centrale Legale e Contenzioso – Group General Counsel, identifica la base giuridica del trattamento tra:

- consenso;
- esecuzione di un contratto di cui l'Interessato è parte o esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- obbligo di legge cui è soggetta la Banca;
- legittimo interesse del Titolare o di terzi cui i dati vengono comunicati, sempre che non prevalgano gli interessi o i diritti e le libertà fondamentali degli Interessati.

Le relative disposizioni operative sono contenute nella "*Guida di Processo Gestione della Conformità – Gestione ambito normativo Tutela della privacy*".

Il trattamento svolto per perseguire un legittimo interesse del Titolare non richiede un consenso, ma soltanto l'Informativa agli Interessati, con puntuale indicazione dei motivi per cui si ritiene che il bilanciamento degli interessi sia a favore del Titolare.

Per stabilire se il trattamento può essere ricondotto al legittimo interesse, il Data Protection Officer, con il supporto della Direzione Centrale Legale e Contenzioso – Group General Counsel, effettua il cosiddetto "test di bilanciamento", ossia valuta:

- che il trattamento sia sufficientemente specifico da poter chiaramente evidenziare la prevalenza degli interessi del Titolare rispetto ai diritti dell'Interessato (es.: quando vi sia il sospetto di una frode ai danni della Banca);
- che il trattamento sia necessario per l'esercizio di un diritto fondamentale o effettuato nell'interesse pubblico, considerando il possibile pregiudizio che deriverebbe per la Banca qualora non effettuasse il trattamento (es.: nel caso di videosorveglianza per motivi di sicurezza);
- che il trattamento rientri nella ragionevole aspettativa dell'Interessato (es.: trattamento per adempiere a richieste dell'autorità di vigilanza e controllo dei rischi operativi e creditizi);
- la sussistenza di un legittimo interesse quando esiste una relazione tra l'Interessato e il Titolare del trattamento (es.: quando l'Interessato è un cliente o è alle dipendenze del Titolare del trattamento) e l'Interessato possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine.

Il **consenso** è **una delle basi giuridiche** che lecitamente possono supportare il trattamento e, pertanto, posta a livello paritetico rispetto alle altre condizioni di liceità del trattamento medesimo.

Il consenso, che può riguardare l'intero trattamento ovvero una o più operazioni dello stesso, per essere valido deve rappresentarsi come libera, specifica, informata ed inequivocabile manifestazione di volontà espressa dall'Interessato, mediante dichiarazione o azione positiva esplicita; per preservare la validità del consenso, il Titolare del trattamento deve adottare modalità di acquisizione dello stesso funzionali a dimostrarne l'esistenza nel tempo e garantire all'Interessato il diritto di revocare il

consenso in precedenza espresso, in qualsiasi momento e con la stessa facilità con cui è stato espresso.

- Se il trattamento riguarda categorie di dati particolari, ossia "*dati che rivelano 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, alla vita sessuale o all'orientamento sessuale della persona*", la richiesta del consenso è obbligatoria a meno che non ricorrano determinati casi, ad esempio, il trattamento[9]: sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare o dell'Interessato in materia di diritto del lavoro e della sicurezza e protezione sociale, nella misura in cui sia autorizzato dal diritto applicabile o da un contratto collettivo ai sensi del diritto vigente;
- riguardi dati personali resi manifestamente pubblici dall'Interessato;
- sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
- sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici sulla base del diritto dell'Unione o nazionale.

Il trattamento, invece, riconducibile a un processo decisionale automatizzato, compresa la profilazione, è lecito se:

- è necessario per l'esecuzione di un contratto o ai fini della conclusione di un contratto di cui l'Interessato è parte;
- è autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare, che identifica le misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'Interessato;
- si basa sul consenso esplicito dell'Interessato.

A seconda delle caratteristiche del trattamento e della base giuridica che lo legittima, il Data Protection Officer verifica che siano fornite agli interessati le informazioni previste, siano richiesti i consensi necessari e sia riconosciuta la possibilità di esercitare i diritti previsti dalla normativa come ad esempio, in caso di trattamento che prevede un processo decisionale automatizzato, il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita e di contestare la decisione.

3.3 Diritto d'accesso ai dati personali ed altri diritti

I diritti riconosciuti all'Interessato dal Regolamento possono essere considerati declinazioni particolari di quel più ampio diritto all'autodeterminazione informativa, che costituisce il perno intorno a cui

[9] Per l'elenco completo di tutti i casi in cui è permesso trattare i dati particolari cfr. art. 9, comma 2, GDPR.

ruotano gli istituti normativi a tutela della protezione dei dati personali. In questo senso, il Regolamento riconosce all'Interessato, ossia alla persona fisica, i seguenti diritti:

- diritto di accesso, ossia il diritto di ottenere la conferma che sia o meno in corso un trattamento di propri dati personali e, in caso affermativo, di ottenerne l'accesso o una copia;
- diritto di rettifica/integrazione dei dati trattati al fine di garantire che siano sempre esatti e aggiornati;
- diritto alla cancellazione dei dati personali oggetto di trattamento;
- diritto di limitazione di trattamento per il periodo di tempo necessario a tutelare i diritti dell'Interessato;
- diritto alla portabilità dei dati[10], ossia il diritto di:
    a) ricevere i dati personali trattati dalla Banca e di conservarli in vista di un utilizzo ulteriore per scopi personali;
    b) trasmettere i dati personali ad un altro Titolare del trattamento;
- diritto di opposizione ai trattamenti basati su un legittimo interesse del Titolare;
- diritto alla revoca del consenso, che deve essere esercitabile con la stessa facilità con cui il consenso è stato prestato;
- diritto di ottenere l'intervento umano, nei casi di decisione basata unicamente su trattamento automatizzato, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita e di contestare la decisione.

Il Regolamento fissa i termini di riscontro alle richieste degli interessati, pertanto il Data Protection Officer, **entro un mese** dal ricevimento della richiesta, fornisce risposta scritta all'Interessato ovvero lo informa, sempre per iscritto, che, in virtù della complessità della richiesta, verrà fornito riscontro entro i successivi due mesi.

Il Regolamento stabilisce che l'esercizio da parte dell'Interessato del diritto d'accesso ai propri dati personali e l'esercizio degli altri diritti previsti nelle Sezioni 3 e 4 è gratuito, salva la possibilità di richiedere all'Interessato, qualora le richieste siano manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, un contributo spese ragionevole, tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta.

([10]) Il diritto alla portabilità dei dati è riconosciuto a condizione che: la base giuridica del trattamento sia il consenso dell'interessato o l'esecuzione di un contratto di cui l'interessato è parte o di misure precontrattuali; il trattamento sia effettuato con mezzi automatizzati.

3.4 Tutela dell'Interessato e risarcimento

L'Interessato può far valere i suoi diritti dinnanzi all'Autorità Garante oppure, in alternativa, dinnanzi all'Autorità Giudiziaria Ordinaria.

Per rivolgersi al Garante l'Interessato dispone di due strumenti, il reclamo e la segnalazione:

- il reclamo consente all'Interessato di lamentare una violazione della disciplina in materia di protezione dei dati personali (art. 77 del Regolamento e artt. da 140-bis a 143 del Codice Privacy) e di richiedere una verifica dell'Autorità;
- la segnalazione è volto a sollecitare un controllo da parte del Garante sulla disciplina in parola.

In entrambi i casi il procedimento amministrativo dinnanzi all'Autorità Garante può condurre all'emanazione dei provvedimenti di cui all'art. 58, comma 2, del Regolamento ovvero, congiuntamente o alternativamente, all'irrogazione di una sanzione amministrativa pecuniaria (ai sensi dell'art. 83 del Regolamento).

Avverso i provvedimenti dell'Autorità Garante, ovvero, alternativamente al ricorso amministrativo, l'Interessato, se ritiene che il trattamento dei dati che lo riguardano non è conforme alle disposizioni della normativa privacy, può proporre un ricorso giurisdizionale dinnanzi all'Autorità Giudiziaria Ordinaria (artt. 78 e 79 del Regolamento). In particolare, sono di competenza dell'Autorità Giudiziaria Ordinaria le controversie relative al risarcimento del danno ai sensi dell'art. 82 del Regolamento e dell'art. 152 Codice Privacy.

Infine, il Codice Privacy, agli artt. da 167 a 172, prevede una serie di illeciti penali connessi alla violazione della disciplina Privacy (quali ad esempio, il trattamento illecito dei dati). La responsabilità penale è sempre personale, pertanto ne risponde esclusivamente la persona fisica (Titolare, Responsabile, Autorizzato) che pone in essere un comportamento illecito.

3.5 Quadro Sanzionatorio

Eventuali violazioni delle disposizioni del Regolamento sono soggette a sanzioni amministrative pecuniarie fino al 4% del fatturato mondiale annuo di Gruppo dell'esercizio precedente, ad esempio:

- violazioni degli obblighi del Titolare e del Responsabile del trattamento, inclusi gli obblighi di sicurezza e di notifica di un *Data Breach,* possono ammontare fino a 10.000.000 di euro o fino al 2% del fatturato annuo;
- violazione dei principi del trattamento, dei diritti degli interessati e inosservanza delle norme in tema di trasferimento di dati personali a terze parti localizzate al di fuori dell'Unione Europea, possono ammontare fino a 20.000.000 di euro o fino al 4% del fatturato annuo.

4 DISPOSIZIONI OPERATIVE

La presente sezione dettaglia gli argomenti e le disposizioni pertinenti alle attività e ai trattamenti svolti dalla Banca ad uso di tutti gli Autorizzati e contiene le relative istruzioni operative dettate al fine di ottemperare alle previsioni del Regolamento.

Tali disposizioni integrano quelle contenute nei seguenti documenti aziendali:

- Linee Guida, Regole e Policy di Sicurezza aziendale, nelle quali sono contenute le politiche aziendali generali di sicurezza e le politiche di sicurezza riferite ad aree specifiche (ad esempio Regole comportamentali di Cybersecurity con annessa adeguata informazione);
- Normativa riferita all'operatività relativa all'utilizzo di sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti (c.d. "S.I.C.") e specifiche lettere di Autorizzazione per gli operatori interessati;
- Normativa riferita all'operatività degli "Amministratori di sistema" e specifiche lettere di Autorizzazione per gli operatori interessati;
- Normativa in materia di Conservazione dei dati personali;
- Ogni ulteriore normativa contenente specifiche disposizioni in tema di trattamento e protezione dei dati personali;
- Lettera di Autorizzazione al trattamento dei dati personali;
- Lettera di Autorizzazione al trattamento dei dati personali relativi a Sistemi di Videosorveglianza.

Con riferimento all'ambito generale della sicurezza informatica, nel documento "*Regole comportamentali di cybersecurity con connessa adeguata informazione*" sono definite le modalità, le regole e le misure di sicurezza ritenute idonee a garantire la protezione del Patrimonio Informativo e dei dati personali trattati dalla Banca a cui il personale dipendente si deve conformare. Al riguardo si evidenzia che, secondo la classificazione delle informazioni riportata nel citato documento[11], le informazioni che contengono Dati Personali sono da classificare almeno con Livello 2 – Riservato.

Tutta la **documentazione riferita alla materia del trattamento e protezione dei dati personali** (GDPR 2016/679 (UE), Codice Privacy D.Lgs. 196/2003 e successivi provvedimenti dell'Autorità Garante, la normativa aziendale ecc.), nonché la **modulistica operativa** richiamata nella presente sezione (informative, consenso ecc.) sono **reperibili nella Intranet aziendale** rispettivamente alla **Sezione Privacy** (tramite il percorso: Gruppo – Governance – Strutture a diretto riporto dei Vertici Aziendali –

([11]) In generale le informazioni devono essere classificate dall'utente su tre diversi livelli di importanza crescente:

- informazioni "ad uso interno";
- informazioni "riservate";
- informazioni "strettamente riservate".

Tutela Aziendale – Privacy), in **ARCO** nelle Sezioni: Normativa–Regole, Documentazione–Modulistica ed in **ARCO-Foreign Network** nelle Sezioni: Operational Guides, Documentation and Communications.

4.1 Autorizzato al trattamento dati

L'Autorizzato è la persona fisica autorizzata dal Titolare o dal Responsabile a compiere operazioni di trattamento di dati personali.

Tutti i dipendenti, senza distinzione di funzione, inquadramento o livello, nonché **tutti i collaboratori dell'azienda** a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, in tirocinio formativo, collaboratori, consulenti ecc.), **sono Autorizzati al trattamento dei dati personali** attinenti e/o comunque connessi alle attività svolte.

A tale riguardo, in conformità al *Provvedimento n. 192 in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie* e come descritto nella normativa aziendale di riferimento "*Regole generali di sicurezza per la protezione del patrimonio informativo*", è stato costituito un sistema di registrazione - tramite log - di ogni operazione di accesso ai dati bancari effettuata da un Autorizzato, e sono stati attivati specifici alert che individuano comportamenti anomali o a rischio relativi alle operazioni bancarie.

È altresì prevista, conformemente al principio di accountability del Titolare, la nomina di specifici Autorizzati, quali ad esempio, quelli incaricati del trattamento dei dati personali relativi a Sistemi di Videosorveglianza o a alla consultazione dei dati relativi ai Sistemi di Informazioni Creditizie (SIC).

Ogni Autorizzato, rispettando gli obblighi di riservatezza e sicurezza imposti dal Regolamento, deve attenersi nel corso dell'attività alle istruzioni impartite dal Titolare e alle disposizioni emanate dalla Banca con le normative aziendali che disciplinano, tempo per tempo, i compiti connessi alle proprie mansioni e che fissano le modalità del trattamento dei dati personali, nonché gli obblighi derivanti da specifiche regole e lettere di autorizzazione.

L'Autorizzato dovrà comunque operare considerando riservati tutti i dati personali e, di norma, soggetti al segreto d'ufficio. Peraltro, già il **segreto bancario** prevede l'obbligo di riserbo sulle operazioni, sui conti e sulle posizioni dei singoli clienti ed è connaturato al rapporto banca-cliente in applicazione dei principi di correttezza e di buona fede nell'esecuzione del contratto; **tale obbligo** di riservatezza **non si esaurisce** allo scadere dell'orario lavorativo né **con la cessazione del rapporto di lavoro.**

L'aggiornamento dell'ambito del trattamento consentito ai singoli Autorizzati e la verifica della sussistenza delle condizioni per la conservazione dei profili abilitativi da parte degli stessi sarà realizzata secondo il criterio del minimo privilegio.

4.1.2 Disposizioni comportamentali

L'Autorità Garante ha più volte evidenziato in tutte le attività che implicano forme di trattamento dei dati personali la primaria importanza dei profili comportamentali rispetto a quelli meramente formali; a tale riguardo gli Autorizzati al trattamento, in generale, **nell'ambito delle attività bancarie** devono:

- aver cura **di far rispettare le "distanze di cortesia"** agli sportelli e nei luoghi dedicati all'esecuzione dell'attività bancaria;
- **evitare telefonate o colloqui con un tono di voce** che possa far udire le informazioni a persone diverse dagli interessati;
- non mostrare le videate del PC ai clienti;
- **fornire informazioni** sui rapporti bancari (es.: saldo, estratto conto, deposito titoli, ecc.) **solo ai titolari di detti rapporti o ai soggetti dagli stessi autorizzati per iscritto e nei limiti dell'autorizzazione**. A titolo esemplificativo, si evidenzia che la semplice conferma dell'esistenza di rapporti di qualsiasi natura fra la Banca ed un soggetto, se data a un terzo che ne abbia fatto richiesta senza esserne autorizzato, costituisce comunicazione di dati personali senza consenso dell'Interessato e, quindi, trattamento illecito di dati personali;
- **evitare l'invio** al cliente di informazioni bancarie **presso recapiti non autorizzati** e accessibili anche a terzi (ad esempio con fax, strumenti di Instant Messaging);
- fornire il **"benefondi"** (inteso quale sola informazione dell'esistenza o meno sul conto corrente del cliente dei fondi necessari al pagamento dell'assegno) **ai soli soggetti legittimati all'incasso** o alla negoziazione dell'assegno e non ad estranei, **evitando accuratamente ogni altra informazione aggiuntiva o commento**;
- prestare la massima cautela nell'accertare l'**esattezza e la completezza dei dati personali** prima di procedere alle segnalazioni alla Centrale d'allarme interbancaria, alle Autorità di Vigilanza, alle Autorità di Pubblica Sicurezza e in generale per tutte le comunicazioni e segnalazioni da effettuare ai sensi delle norme vigenti;
- verificare la completezza e l'esattezza dei dati trattati nell'eseguire gli ordini di pagamento impartiti dai clienti nell'ambito degli accordi interbancari (Sepa Direct Debit - SDD);
- **evitare di acquisire più volte copie di documenti** già disponibili agli atti;
- informare la clientela in ordine alle **registrazioni telefoniche**, anche se già previste nel testo dei contratti di erogazione dei servizi;

- porre la massima attenzione nell'imbustamento della corrispondenza e nell'invio di comunicazioni elettroniche al fine di **evitare che vengano inviati** a clienti **documenti non di pertinenza**;

- curare che i **fascicoli, le notizie e le informazioni** di qualunque tipo, contenenti dati personali, disponibili nella propria struttura operativa, **non siano accessibili a soggetti non autorizzati, né fisicamente** (ad es.: documenti lasciati incustoditi sulla scrivania o su scaffali dell'ufficio), **né informaticamente** (ad es.: dati accessibili sul PC o su cellulari non bloccati in caso di allontanamento temporaneo dalla postazione di lavoro)[12];

- **è vietato creare banche dati**/liste contenenti dati personali ovvero conservare dati personali al **di fuori di quanto espressamente autorizzato** per l'ambito della propria funzione.

Per le specifiche attività di **recupero crediti** gli Autorizzati al trattamento devono:

- **garantire** nei contatti personali col cliente debitore **la riservatezza del colloquio**, che deve svolgersi in locali della Banca alla presenza del solo personale incaricato di gestire il rapporto, evitando per quanto possibile incontri a domicilio o sul luogo di lavoro dell'Interessato;

- **verificare** preliminarmente, in caso di contatti telefonici, **che l'interlocutore sia effettivamente l'Interessato** (in caso di incertezza sull'identità, l'intervento sarà limitato ad un semplice invito a recarsi in filiale per comunicazioni). È fatto divieto di ricorrere a comunicazioni telefoniche preregistrate volte a sollecitare il pagamento, realizzate senza l'intervento di un interlocutore autorizzato, essendo tale modalità suscettibile di rendere edotti soggetti diversi dal debitore della sua condizione di inadempimento. È fatto altresì divieto di inviare messaggi SMS o lasciare messaggi di sollecitazione nella segreteria telefonica di utenze fisse o mobili dei clienti, attraverso i quali si comunichi l'esposizione debitoria o la necessità di recarsi in filiale per ripianare l'esposizione;

- prestare la massima cura, ove si renda necessario inviare una **comunicazione scritta** (sollecito o costituzione in mora, secondo quanto prescritto dalla normativa interna), a che il **plico** sia sempre **ben sigillato** e rechi il **solo nome, cognome e indirizzo del cliente**, e che non renda in alcun modo palese il contenuto della comunicazione (ad esempio tramite cartoline postali o plichi recanti all'esterno la scritta "recupero crediti");

Con riferimento alle specifiche attività conferite a **Filiali On Line** (FOL) e **Filiale Remota**, qualora dalle verifiche effettuate gli operatori autorizzati rilevino elementi di incertezza o dubbi sulla corretta identità del cliente con cui si stanno relazionando, non devono fornire informazioni sui rapporti bancari, ma devono invitare lo stesso a presentarsi in filiale.

([12]) Vedasi il documento di "*Regole comportamentali di cybersecurity con annessa adeguata informazione*".

In tale contesto assumono particolare rilevanza le ***regole comportamentali in materia di cybersecurity***[13]. A titolo esemplificativo e non esaustivo si ricordano di seguito alcune regole specifiche previste da tale documento:

- gestire in **sicurezza user-ID** e componenti riservate (ad esempio, password o PIN) che permettono l'accesso agli strumenti informatici di lavoro;
- impedire l'accesso a dati e programmi effettuando il blocco temporaneo quando uno strumento acceso non viene utilizzato (**clean screen**);
- porre **attenzione all'ambiente circostante** per evitare situazioni di shoulder surfing in caso di utilizzo degli strumenti informatici in luoghi pubblici;
- trasportare gli strumenti informatici di lavoro in modo adeguato e avendo cura di **non lasciarli mai incustoditi in luoghi pubblici** o non adeguatamente protetti; in particolare, nel caso di viaggi di lavoro gli utenti devono: tenerli sempre con sé ed evitare di lasciarli incustoditi in automobile (anche se chiusa a chiave);
- nell'utilizzo della posta elettronica **indicare il livello di classificazione delle informazioni** contenute nel testo del messaggio e/o negli allegati, utilizzando ove presenti le funzionalità messe a disposizione dall'applicativo di posta;
- prestare **attenzione ai messaggi** di posta elettronica e a file, programmi e oggetti allegati ricevuti **da mittenti sconosciuti**, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo;
- nella **condivisione di documenti elettronici** ove possibile adottare **contromisure di protezione** (ad esempio, utilizzando funzioni che permettano la sola lettura o limitino la possibilità di modifica).

4.2 Assicurare la conformità alla protezione dei dati sin dalla progettazione (Privacy by Design)

Nel momento in cui si **individua una nuova iniziativa** (come **nuovi prodotti o servizi**, iniziative di outsourcing, modifiche organizzative, operazioni societarie) o si **intende apportare una modifica ad un trattamento di dati personali già in essere**, sia esso nei confronti dei clienti o del personale dipendente, deve essere avviato il processo di Privacy by Design volto, nell'ambito dell'accountability del Titolare, alla determinazione delle logiche di protezione dei dati personali attraverso

(13) Vedasi il documento di "*Regole comportamentali di cybersecurity con annessa adeguata informazione*" al cui interno sono previste ulteriori indicazioni che possono mitigare il rischio di perdita e/o diffusione di dati aziendali.

l'**individuazione dei potenziali rischi di non conformità** e delle **misure tecniche ed organizzative idonee per mitigare tali rischi lungo l'intero ciclo di vita del trattamento**.

Nell'ambito del processo di Privacy by Design, la **Funzione di business e di supporto** che promuove la nuova iniziativa o la modifica di un trattamento già esistente deve **provvedere alla raccolta delle relative informazioni** indicate nella specifica modulistica di processo e alla trasmissione al Data Protection Officer. Nel caso in cui all'interno dell'iniziativa sia coinvolto un Fornitore/Terza parte andranno, inoltre, raccolte e trasferite al Data Protection Office anche le informazioni afferenti alle attività di detta società, in modo da permetterne la determinazione del ruolo soggettivo (corrispondente a Titolare o Responsabile o Contitolare) e i relativi obblighi contrattuali, come dettagliato al cap. 4.5 del presente documento.

Nell'ambito del processo di Privacy by Design, il Data Protection Officer effettua una valutazione di legittimità del trattamento ed effettua una valutazione dei rischi potenziali per i diritti e le libertà degli interessati con l'ausilio di checklist, dell'eventualmente Test di bilanciamento e degli strumenti di valutazione delle misure di sicurezza[14] (c.d. Privacy Impact Assessment).

L'output di tale valutazione è la determinazione del profilo di rischio residuo del trattamento quale: basso, medio, alto. Qualora la valutazione evidenzi un rischio residuo basso o medio la Funzione di business e di supporto può avviare il trattamento e procedere all'aggiornamento del Registro dei Trattamenti; se invece il **rischio residuo risulta alto** la Funzione di business e di supporto dovrà decidere se **effettuare una consultazione preventiva all'Autorità Garante oppure non intraprendere il trattamento**. **L'eventuale richiesta di consultazione al Garante viene formalizzata dal DPO** tramite la relazione sul Privacy Impact Assessment svolto; a seguito del riscontro dell'Autorità Garante, previsto entro otto settimane dal ricevimento della richiesta, la Funzione di business e di supporto verifica la fattibilità delle istruzioni ricevute dall'Autorità e valuta conseguentemente se avviare o non intraprendere il trattamento.

Il **DPO attua un'attività di monitoraggio delle decisioni** della Funzione di business e di supporto nel procedere al trattamento, ovvero dell'implementazione delle eventuali raccomandazioni espresse, secondo il Report di Privacy by Design, Privacy by Default e Privacy Impact Assessment[15] e, almeno annualmente, riferisce[16] al Consiglio di Amministrazione anche in merito a tali attività di monitoraggio.

([14]) Si vedano i documenti contemplati dalla "*Guida di Processo Gestione della Conformità – Gestione ambito normativo Tutela della privacy*" come: Lawfulness Matrix, Test di bilanciamento del legittimo interesse del Titolare, Metodologia PIA.

([15]) Trattasi di documento di raccordo delle analisi effettuate durante l'istruttoria di Privacy by Design, in cui il DPO esprime la sua valutazione in merito alla limitazione delle finalità del trattamento e la relativa base giuridica, nonché dei rischi potenziali.

([16]) Mediante la Relazione annuale di sintesi sull'attività svolta ai sensi del Regolamento UE 2016/679.

4.3 Liceità del trattamento e l'acquisizione del Consenso dell'Interessato

Coerentemente con il Regolamento e con quanto rappresentato al cap. 3.2 del presente documento, la Banca presidia, nell'ambito del Processo di privacy by design, il rispetto dei principi del GDPR e, in particolare, del principio di liceità dei trattamenti dei dati personali del cliente effettuati nell'ambito dell'erogazione di servizi bancari e finanziari richiesti dall'Interessato; il trattamento dei dati dev'essere strettamente connesso e strumentale:

- alla gestione dei rapporti con l'Interessato o delle operazioni richieste che abbiano natura contrattuale, ovvero, in generale, dei servizi continuativi od occasionali resi allo sportello, a distanza o fuori sede;
- all'esecuzione dei connessi obblighi di legge, come ad esempio gli adempimenti di identificazione ed adeguata verifica ai fini della normativa antiriciclaggio.

La Banca individua nel consenso, liberamente espresso, in forma specifica e documentata (ad esempio attraverso la sottoscrizione di un modulo cartaceo oppure in formato elettronico, tramite firma grafometrica o tramite firma digitale), la base giuridica dei **trattamenti Commerciali riportati nell'Informativa nei confronti di persone fisiche ai sensi dell'art. 13 e 14 del Regolamento (UE) 2016/679:** ovvero per attivare trattamenti funzionali alle attività di marketing[17] della Banca e del Gruppo, come di seguito evidenziato:

- prestazione di consenso ai fini di informazione commerciale, offerte dirette, indagini di mercato o di customer satisfaction relative a prodotti e servizi della Banca e di società del Gruppo Intesa Sanpaolo: se il cliente nega tale consenso, la Banca non potrà svolgere le attività in oggetto, né l'attività di rilevazione del grado di soddisfazione del cliente;
- prestazione di consenso ai fini di offerta di prodotti e servizi della Banca e delle società del Gruppo Intesa Sanpaolo specificamente individuati in base al profilo personale: se il cliente nega tale consenso, la Banca non potrà attivare azioni di promozione commerciale nei confronti del cliente stesso preventivamente "profilato" ovvero attraverso l'elaborazione dei dati personali relativi a preferenze, abitudini, scelte di consumo e altre informazioni acquisite;
- prestazione di consenso ai fini di informazione commerciale, offerte dirette, indagini di mercato o di customer satisfaction relative a prodotti e servizi di altre società: se il cliente nega tale consenso, la Banca non potrà attivare azioni o mailing promozionali per proporgli prodotti e servizi (polizze assicurative, prodotti finanziari, ecc.) di società terze.

[17] Gli eventuali consensi Commerciali rilasciati decadono al momento della chiusura di tutti i rapporti in essere con la Banca.

4.3.1 Sottoscrizione del consenso

Il consenso deve essere sottoscritto, anche in forma elettronica, dal cliente (persona fisica) interessato dal trattamento dei propri dati personali anche nel caso di persone fisiche collegate a persone giuridiche, enti ed associazioni, quando queste vengono censite nelle basi dati aziendali in qualità di legali rappresentanti od a qualsiasi altro titolo[18].

Per i soggetti interessati riconducibili a particolari tipologie di clientela la sottoscrizione del consenso deve avvenire nel rispetto della normativa in materia di poteri di firma e di rappresentanza.

Per le persone giuridiche, gli enti o le associazioni, il consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto[19] deve essere sottoscritto dal legale rappresentante.

In generale, **l'inerzia dell'Interessato a scegliere** se prestare o negare il proprio consenso **deve considerarsi**, a tutti gli effetti, come una **"negazione di consenso"**, il campo relativo al consenso non espresso deve essere lasciato vuoto e, anche in tale caso, deve essere sottoscritto dall'Interessato, al fine di comprovare il ricevimento dell'Informativa.

Al cliente deve essere sempre consegnata una copia, in formato cartaceo o elettronico, dell'informativa e dei consensi dallo stesso espressi.

4.3.1.1 Consenso dei minori

I **minori** meritano una **specifica protezione** relativamente ai dati personali che li riguardano, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate, nonché dei loro diritti in relazione al trattamento dei dati personali.

([18]) In riferimento al trattamento dei dati personali è richiesto il **consenso per la finalità di marketing diretto ed indiretto** quali:

- informazione commerciale, offerte dirette, indagini di mercato o di customer satisfaction relative a prodotti e servizi relative a prodotti e servizi della Banca e di società del Gruppo Intesa Sanpaolo;
- offerta di prodotti e servizi della Banca e di società del Gruppo Intesa Sanpaolo specificamente individuati in base al profilo personale;
- informazione commerciale, offerte dirette, indagini di mercato o di customer satisfaction relative a prodotti e servizi di altre società.

Inoltre, in relazione al **trattamento delle categorie particolari di dati personali** è richiesta una **manifestazione esplicita di consenso** per l'erogazione di specifici servizi e prodotti quali la stipula di finanziamenti assistiti da polizze assicurative, la stipula di polizze assicurative e l'erogazione di servizi di welfare.

([19]) *Provvedimento del Garante sul "Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto"* del 15 maggio 2013 (pubblicato sulla Gazzetta Ufficiale n. 174 del 26 luglio 2013).

Qualora il trattamento trovi la propria base giuridica nel consenso dell'Interessato (di cui all'art. 6.1, lettera a), questo è lecito soltanto se e nella misura in cui sia prestato o autorizzato dal **titolare della responsabilità genitoriale sul minore**.

Al compimento della maggiore età i consensi precedentemente espressi andranno **nuovamente raccolti,** interpellando l'Interessato diventato maggiorenne.

4.3.2 Modifica del consenso

Il cliente può, in ogni momento, modificare le proprie espressioni di consenso, decidendo di conferire un consenso prima negato, o di revocarne uno dato.

La variazione può essere disposta dal cliente direttamente nell'apposita sezione dell'Internet Banking o della App della Banca, se ha aderito a questi servizi, oppure può essere richiesta dal cliente, sia in forma libera che mediante apposito modulo di esercizio dei diritti[20], e può essere presentata direttamente in Filiale, inviata tramite posta tradizionale, e-mail o scrivendo al DPO.

Accertato che il richiedente abbia titolo ad esercitare la richiesta, secondo il processo descritto nella "*Guida di Processo sulla Gestione della Conformità ambito normativo Tutela della privacy*", se la richiesta è pervenuta al Gestore e/o all'Assistente, questi provvedono ad evaderla senza ingiustificato ritardo con le consuete modalità operative, utilizzando i sistemi informativi a supporto. Se la richiesta è pervenuta al Data Protection Officer, questi provvede a richiedere alla Funzione Sistemi Informativi o altre strutture responsabili del trattamento di procedere alla revoca del consenso sui sistemi informativi coinvolti.

4.3.3 Archiviazione del consenso

In caso di sottoscrizione del consenso in formato elettronico (tramite firma grafometrica o firma digitale remota) viene attivato un processo di archiviazione informatica della documentazione, così come descritto nella normativa aziendale di riferimento "*Guida di Processo Processi Amministrativi - Archiviazione in formato cartaceo ed elettronico dei documenti*".

I moduli di consenso in formato cartaceo devono essere conservati in ordine cronologico in apposito e separato dossier, presso la Filiale o Unità Organizzativa dove l'Interessato è stato registrato. Ne consegue che il modulo di consenso firmato dal cliente deve essere conservato presso la Filiale o Unità Organizzativa. Per le restanti modalità di conservazione dei documenti si rimanda alla "*Guida di Processo Processi Amministrativi - Archiviazione in formato cartaceo ed elettronico dei documenti*".

[20] Il Modulo è disponibile sul sito web della Banca o può essere richiesto al Gestore in filiale.

4.4 Resa dell'informativa agli interessati

Per garantire un trattamento corretto e trasparente è necessario, come previsto dal Regolamento, rendere disponibile agli Interessati una serie di informazioni in modo conciso, trasparente, intellegibile, facilmente accessibile e dal linguaggio semplice e chiaro.

Si riportano nel seguito i contenuti delle principali Informative alla base dei rapporti intrattenuti con la clientela, al fine di illustrarne la struttura complessiva. La relativa modulistica operativa è accessibile in **ARCO** nella Sezione "Documentazione-Modulistica-Compliance_e_Adempimenti_di_Legge-Tutela Aziendale_Privacy" ed in **ARCO-Foreign Network** nella Sezione "Documentation and Communications".

Informativa nei confronti di persone fisiche ai sensi dell'art. 13 e 14 del Regolamento (UE) 2016/679: Informativa generale di riferimento, da fornire al cliente (persona fisica), continuativo o occasionale, al momento della raccolta dei dati personali (ad esempio, in occasione dell'apertura di rapporti bancari o dell'esecuzione di operazioni occasionali allo sportello) a cura dell'Autorizzato che effettua tale attività.

L'Informativa, in conformità con il Regolamento, contiene, tra l'altro, le seguenti informazioni:

- il Titolare del trattamento dei dati personali;
- dati di contatto del Responsabile della Protezione dei dati (DPO);
- le categorie di dati trattati, le fonti di acquisizione, le finalità del trattamento e la base giuridica che legittima il trattamento, ovvero la necessità del rilascio dei dati e le conseguenze del loro mancato conferimento;
- le categorie dei soggetti ai quali i dati possono essere comunicati per le finalità strettamente connesse e strumentali alla gestione dei rapporti con la clientela ovvero per le finalità funzionali all'attività della Banca;
- l'eventuale trasferimento dei dati ad un Paese terzo o ad un'organizzazione fuori dall'Unione Europea;
- le modalità di trattamento e i tempi di conservazione dei dati;
- i diritti dell'Interessato, di cui alle Sezioni 3 e 4 del Regolamento e la modalità di esercizio degli stessi; l'esistenza del diritto di revocare il consenso in qualsiasi momento qualora il trattamento dei dati personali si basi su detta condizione.

Detta Informativa 'standard persone fisiche' deve essere sempre resa alle persone fisiche collegate a persone giuridiche, enti ed associazioni, quando queste vengono censite nelle basi dati aziendali in qualità di legali rappresentanti od a qualsiasi altro titolo.

Informativa nei confronti di persone giuridiche, enti o associazioni: per le persone giuridiche, enti o associazioni il Regolamento non stabilisce l'obbligo di Informativa; tuttavia secondo il Codice Privacy (art. 130) per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale effettuati sia con sistemi automatici di comunicazione sia con le c.d. "comunicazioni elettroniche"[21] (posta elettronica, telefax, SMS, MMS, ecc.) – anche non automatizzate – è previsto che venga acquisito il consenso. Pertanto, al fine di poter rappresentare tale situazione alla clientela di riferimento, è stata redatta una breve formula di Informativa per tali soggetti.

Informativa ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679 e dell'art.6 del Codice di Condotta per i Sistemi Informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti: trattasi di Informativa specifica predisposta secondo un 'modello di riferimento' stabilito nel Provvedimento del Garante in materia di Sistemi di informazione creditizia, da fornire al cliente (persona fisica e quindi, oltre che in veste di 'consumatore', anche ai sensi degli artt. 4 e 8 del Codice di condotta per i SIC come "esponente aziendale, partecipante al capitale sociale o soggetto collegato dalla società richiedente") al momento della richiesta di un rapporto di credito nonché agli eventuali interessati coinvolti nella richiesta stessa nelle vesti di coobbligati e garanti. Con riferimento specifico alla sua formulazione si sottolinea in particolare la manifestazione dei termini di conservazione dei dati sui SIC, sia di tipo positivo che negativo.

Informativa clienti prospect: è resa all'Interessato che si configura come cliente potenziale; viene utilizzata in occasione della raccolta di dati di soggetti che non sono titolari di rapporti con la Banca, ad esempio in occasione della formulazione di un'offerta commerciale a cura del Gestore di filiale, oppure tramite una procedura automatica in occasione dell'accesso dell'interessato al sito vetrina del Gruppo per effettuare simulazioni di acquisto dei prodotti vendibili online e che successivamente effettua la registrazione alla Guest Area dedicata, nonché nell'ambito di iniziative approvate dalle Direzioni Regionali o da altre Strutture della Banca, come dei concorsi a premi abbinati alle sponsorizzazioni.

Informativa sui sistemi biometrici per il controllo accessi e/o **Informativa sui sistemi videosorveglianza** afferenti le Filiali: viene resa in presenza di sistemi biometrici per il controllo degli accessi e/o di sistemi di videosorveglianza e/o di videoregistrazione digitali o analogici posti all'ingresso della Filiale o al suo interno. Il responsabile della Unità Organizzativa (c.d. U.O.G.), individuato anche quale specifico Autorizzato per il trattamento dei dati relativi alla videosorveglianza, attraverso l'esposizione di appositi cartelli (esterni ed interni), collocati in modo ben visibile in prossimità delle apparecchiature e

---

([21]) *Provvedimento del Garante del 20 settembre 2012 in ordine all'applicabilità alle persone giuridiche del codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011; Linee Guida in materia di attività promozionale e contrasto allo spam - 4 luglio 2013* (Pubblicato sulla Gazzetta Ufficiale n. 174 del 26 luglio 2013); *Provvedimento sul "Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto"* del 15 maggio 2013 (pubblicato sulla Gazzetta Ufficiale n. 174 del 26 luglio 2013).

riportanti le informative previste dal Garante, deve comunicare agli utenti che accedono alla filiale l'esistenza di tali sistemi, le finalità perseguite, le limitazioni all'accesso ai dati contenuti e le modalità di esercizio dei propri diritti. Se una persona rifiuta di sottoporsi alla lettura dell'impronta digitale entrando in locali assistiti da sistemi di videosorveglianza abbinati ad impianti di rilevazione biometrica, occorre comunque garantire alla stessa l'accesso in filiale con modalità alternative. Analogo comportamento deve essere tenuto per i locali di sede centrale o altri locali aperti al pubblico da parte dei soggetti preposti.

Informativa sui sistemi di controllo accessi biometrici alle aree riservate: viene resa nel caso di acquisizione di dati personali biometrici finalizzati a generare il template delle impronte digitali dell'interessato ed all'emissione di un badge contente il template stesso necessario unicamente per accedere alle aree riservate della Banca.

Informativa sulla sottoscrizione di documenti con firma grafometrica: la Banca adotta il servizio di firma grafometrica che consente di sottoscrivere i documenti bancari in formato elettronico, attraverso la registrazione informatica dei parametri della firma autografa (ad esempio: velocità, pressione, inclinazione, ecc.) apposta dal cliente su uno specifico dispositivo (tablet). All'atto di adesione al servizio è necessario rendere all'Interessato un'apposita Informativa in ordine alle finalità e alle modalità del trattamento dei dati, con particolare riguardo al ruolo del soggetto Terzo Fiduciario nel procedimento di accesso al modello grafometrico (consentito nei soli casi di contenzioso o a seguito di richiesta dell'Autorità Giudiziaria). Le disposizioni operative sono contenute nella "*Guida di Processo Servizi di accesso a distanza e di dematerializzazione – Servizi di Identificazione e Riconoscimento a distanza*" capitolo "*Firma Grafometrica Del Cliente – Sottoscrizione della Documentazione Prodotta Dalla Banca In Formato Elettronico*".

Informativa per i visitatori di sedi, palazzi e uffici: fornita dall'Autorizzato agli Interessati qualora si proceda all'identificazione e registrazione dei soggetti esterni che accedono ai locali della Banca.

Informativa per i fornitori: nell'ambito della conclusione di contratti con i soggetti fornitori della Banca è necessario rendere a tali soggetti (persone fisiche) la specifica Informativa. Tale Informativa viene altresì rilasciata all'atto dell'iscrizione al portale informatico dedicato alla gestione dei fornitori.

Informativa cookie: fornita agli interessati nell'ambito dell'accesso e navigazione delle soluzioni web della Banca (quali sito internet ed App), comprensiva della descrizione dei differenti cookie previsti[22], delle relative basi giuridiche nonché dei periodi di attività.

Informativa per dipendenti e assimilati: fornita a tutto il personale nell'ambito del rapporto professionale e predisposta in sinergia con la Direzione Centrale Affari Sindacali e Politiche del Lavoro.

([22]) Nel set dei cookie di profilazione sono identificati quelli gestiti dalla Banca quale Titolare, da quelli gestiti da altre Terze Parti. In riferimento a questi ultimi viene reso il collegamento alle pagine *web* contenenti le informative e i moduli per l'acquisizione del consenso delle relative terze parti.

Informative candidature professionali: fornita a tutti gli interessati che intendono candidarsi per posizioni professionali e predisposta in sinergia con la Direzione Centrale Affari Sindacali e Politiche del Lavoro.

Più in generale si rappresenta che **ulteriori Informative** possono essere individuate e finalizzate con il DPO nell'ambito di un processo di Privacy by Design. A titolo indicativo e non esaustivo, come Informative da predisporre in modo puntuale vi sono quelle per:

- **l'acquisizione di dati personali da terze parti quali società o fonti pubbliche:** nel caso di acquisizione di dati personali da società terze o da fonti pubbliche ovvero non direttamente dall'Interessato, occorre fornire allo stesso, non oltre la prima comunicazione, l'Informativa sul trattamento dei dati, in cui si specifichi la fonte da cui sono stati acquisiti i dati personali;

- **le iniziative commerciali o promozionali:** a fronte di iniziative commerciali e promozionali di tipo occasionale, quali ad esempio partecipazione a concorsi a premi, contatti da siti web, vendita o prenotazione di biglietti per avvenimenti culturali o sportivi, ecc. che prevedano finalità specifiche di trattamento dati;

- **le operazioni di cessione di credito:** per le operazioni di cartolarizzazione, cessione di crediti di impresa (factoring) e di cessione di crediti in blocco (ad es. cessione sportelli).

4.5 Affidamento a terze parti di attività comportanti il trattamento dati

Nel caso in cui l'affidamento di un'attività ad un Fornitore/Terza parte comporti il trattamento di dati personali (indipendentemente che questi afferiscano a clienti, dipendenti, ecc.), si rende necessario, con le modalità indicate nella "*Guida di Processo Gestione della Conformità - Gestione ambito normativo Tutela della privacy*" e, ove ne ricorra l'ipotesi, nella "*Guida di Processo Outsourcing - Esternalizzazioni extragruppo e infragruppo non in attuazione del modello di Gruppo*", prima di conferire l'incarico, che l'Ente Richiedente attivi il Data Protection Officer affinché valuti:

- il ruolo soggettivo (Titolare, Contitolare, Responsabile) da attribuire alla Terza parte;
- la presenza di un subaffidatario, preventivamente e specificatamente autorizzato;
- le adeguate garanzie in caso di trasferimento dei dati al di fuori dell'Unione Europea.

Nel caso in cui il contratto in fase di stipula con il Fornitore/Terza parte (che riveste il ruolo di Responsabile del Trattamento) comporti una sub-fornitura, il subaffidamento andrà preventivamente e specificamente autorizzato dall'Ente Richiedente e dall'Ente di Acquisto (ciascuno per i rispettivi ambiti di competenza), previo censimento dei subaffidatari sul Portale Fornitori. Resta comunque fatta salva l'ipotesi di una preventiva autorizzazione generale in forma scritta, fermo restando che in tale ultimo caso il Fornitore/Terza parte dovrà comunicare tempestivamente eventuali aggiunte o sostituzioni dei subaffidatari in modo da consentire alla Banca di opporsi. In ogni caso il Fornitore/Terza parte conserverà la responsabilità dell'adempimento degli obblighi che gravano su ciascun subaffidatario coinvolto.

In caso di comunicazione di dati personali a un Fornitore/Terza parte qualificato come Titolare, il Data Protection Officer valuta, con il supporto della Direzione Centrale Legale e Contenzioso Group General Counsel, la presenza di una base giuridica idonea a legittimare la comunicazione dei dati personali (consenso degli interessati, esecuzione di un contratto tra Interessato e Titolare o di misure precontrattuali adottate su richiesta dell'Interessato, ecc.).
Ove stabilito per il Fornitore/Terza parte il ruolo soggettivo di Responsabile, questi riceverà, tramite l'Ente Richiedente o l'Ente d'Acquisto, la lettera di Nomina a Responsabile recante le istruzioni da adempiere per il trattamento dei dati in esecuzione del contratto.

Alla luce del ruolo soggettivo determinato per la Terza parte come Titolare, Responsabile o Contitolare del trattamento dei dati personali verrà tempestivamente aggiornato, a cura della Direzione Centrale Tutela Aziendale, l'elenco dei soggetti terzi che trattano dati personali, e disposta la pubblicazione in ARCO nella Sezione: Documentazione-Modulistica-Compliance_e_Adempimenti_ di_ Legge-Tutela _Aziendale – Privacy, affinché possa essere prontamente reperibile in caso di richiesta degli interessati come indicato nell'informativa nei confronti di persone fisiche ai sensi dell'art. 13 e 14 del Regolamento (UE) 2016/679.

4.6 Affidamento a terze parti di attività di trattamento dati tramite contatto telefonico

Sulla base della delibera dell'Autorità per le Garanzie nelle Comunicazioni (AGCom) n.666/08/CONS del 26.11.2008 e di quanto sancito dall'Articolo 1, comma 243, della Legge n. 232 del 2016 (c.d. "Legge di bilancio"), tutti gli operatori economici che svolgono attività di call center, nonché i soggetti terzi affidatari dei servizi di call center, siano esse inbound che outbound, sono tenuti a trasmettere domanda di iscrizione al Registro degli operatori di comunicazione (c.d. "R.O.C.") e a rispettare gli obblighi previsti dal regolamento allegato alla delibera n. 666/08/CONS.

In particolare, tra gli obblighi del Regolamento si segnala che l'Interessato, per tramite dell'operatore, debba essere informato preliminarmente in merito al Paese in cui è fisicamente collocato l'operatore (Territorio nazionale, Paesi UE, Paesi extra UE).

Le violazioni alle disposizioni del Regolamento sono comunicate dal Ministero dello Sviluppo Economico (MISE) all'Autorità Garante.

4.7 Termini di Conservazione dei dati personali

Il Regolamento annovera tra i principi applicabili al trattamento dei dati il così detto "principio della limitazione della conservazione". In particolare, l'art. 5, comma 1 lett. e) dispone espressamente che i dati siano conservati in una forma che consenta l'identificazione degli interessati per un **arco temporale strettamente necessario al conseguimento delle finalità** per le quali sono trattati; periodi più lunghi di conservazione sono consentiti esclusivamente per finalità di archiviazione e pubblico interesse, di ricerca scientifica, storica o statistica. Tale principio è direttamente discendente da quello

della minimizzazione del trattamento. Infatti, dalla necessità che i dati personali debbano essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento, discende l'obbligo di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il Titolare del trattamento deve stabilire un termine per la cancellazione. La cancellazione dei dati personali alla scadenza del periodo previsto costituisce quindi un adempimento espressamente prescritto dal Regolamento (in tal senso si esprime il considerando n. 39).

Dalla cogenza di tale principio deriva l'obbligo per il Titolare di fornire, nell'Informativa resa all'Interessato, tutte le informazioni necessarie a garantire la liceità e la trasparenza del trattamento, tra cui l'indicazione del periodo di conservazione dei dati o, se ciò non risulta possibile, i criteri utilizzati per determinare tale periodo (artt. 13 e 14, comma 2, lettera a).

La determinazione dei termini di conservazione può avvenire in base ad un obbligo normativo o, in assenza di specifica norma, in base ad una valutazione del Titolare (la Banca).

Quanto agli obblighi normativi, alcune disposizioni legislative prescrivono specifici termini di conservazione. Il Codice Civile (art.2220) individua, ad esempio, un termine di conservazione della documentazione di dieci anni (cfr. anche art. 119, comma 4, Tub). Generalmente, il suddetto termine decennale trova applicazione rispetto ai dati personali acquisiti nell'ambito di rapporti contrattuali di cui la Banca è parte: così, ad esempio, nei contratti bancari (conto corrente), nei contratti di finanziamento (mutui e finanziamenti), nei contratti di lavoro e nei contratti con i fornitori. Tale termine decorre dalla chiusura del rapporto/dall'operazione; in presenza di atti interruttivi (ad es. un atto di citazione), il termine si interrompe e inizia nuovamente a decorrere una volta che l'evento interruttivo sia cessato.

Rispetto a specifici prodotti o servizi erogati dalla Banca possono, peraltro, trovare applicazione normative specifiche. Così, ad esempio, rispetto ai servizi di canale venduti unitamente al servizio di firma elettronica avanzata o digitale (es. My Key, My Business, …), il termine di conservazione è pari a 20 anni dalla sottoscrizione del contratto (art. 32 Codice dell'Amministrazione digitale, art. 57 comma 1 DPCM 22/02/2013).

Termini brevi di conservazione sono invece previsti con riferimento ai dati anagrafici dei clienti *Prospect*, rispetto ai quali il termine di conservazione è di 18 mesi dal censimento dell'Interessato; in tali termini si è espresso anche il Garante della Privacy con il *Provvedimento del 24 febbraio 2005*, così come relativamente alle registrazioni di videosorveglianza finalizzate alla sicurezza fisica, rispetto ai quali il termine massimo di durata della conservazione dei dati è limitato *"ai sette giorni successivi alla rilevazione delle informazioni*" (in tal senso si è espresso il Garante della Privacy nel *Provvedimento dell'8 aprile 2010*). Nei casi residuali, in cui il termine di conservazione non è espressamente previsto da una norma primaria o regolamentare, compete al Titolare giustificare e documentare il termine ritenuto più congruo, tenendo in debito conto il principio di minimizzazione che si applica al trattamento dei dati.

Nell'ambito di tale valutazione, il Titolare può prendere in considerazione, ad esempio, il termine di prescrizione decennale entro il quale un cliente può esperire azione giudiziaria nei confronti del medesimo. In tal caso, la finalità di conservazione dei dati per un periodo di dieci anni è individuata nell'interesse del Titolare ad agire in sede giudiziaria per la tutela dei propri diritti (art. 2946 C.C. secondo il quale i diritti si estinguono per prescrizione con il decorso di dieci anni).

Per una disamina più dettagliata dei termini di conservazione dei dati previsti per ciascun rapporto di cui la Banca è parte si rimanda al documento aziendale "*Regole in materia di conservazione dei dati personali*".

4.8 Segnalazione di trattamento di dati personali non autorizzato e Data Breach

In conformità a quanto disposto dall'Autorità Garante nel *Provvedimento n.192 del 2011 "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie"* art. 4.3, e *nel* GDPR *Sezione 2 "Sicurezza dei dati personali", art. 32 " Sicurezza del trattamento",* ogni Autorizzato, appena avuta conoscenza di un trattamento di dati personali anomalo o illecito, deve **segnalare immediatamente** l'accaduto alle Funzioni di Incident Management competenti[23], ossia a tutte quelle Funzioni incaricate della risoluzione delle problematiche connesse alle risorse aziendali e alle attività operative e/o di business di cui sono responsabili, come previsto nell'ambito della "*Guida di Processo Gestione degli Eventi Critici*". Nel caso in cui sia un Fornitore/Terza parte a segnalare un *Data Breach,* questi, in qualità di Responsabile del trattamento, è tenuto a riportarlo senza ingiustificato ritardo alla struttura indicatagli nella lettera di Nomina a Responsabile del trattamento dei dati tramite l'accurata compilazione della modulistica fornita a corredo del documento di nomina (c.d. "*Information Set*").

([23]) A titolo esemplificativo e non esaustivo, si riporta di seguito l'elenco delle Funzioni di Incident Management, ossia quelle Funzioni che si attivano per il superamento delle problematiche connesse alle risorse aziendali e alle attività operative e/o di business di cui sono responsabili:

- Direzione Centrale Sistemi Informativi;
- Security Operation Center (SOC);
- Security Fraud Prevention;
- Data Protection Officer (DPO);
- Sicurezza Fisica;
- Direzione Centrale Immobili e Logistica;
- Referenti del piano settoriale di BCM.

Il Data Protection Officer, in qualità di figura competente, valuta la necessità di segnalazione del *Data Breach* all'Autorità Garante e verso l'interessato, qualora necessario, e provvede al relativo invio della segnalazione secondo termini e modalità previste[24].

4.9 Esercizi dei diritti dell'Interessato

L'Interessato – o, per conto dello stesso, un soggetto terzo munito di delega (anche su carta semplice es. delegato/procuratore, studio legale, associazione di categoria) o un rappresentante legale dello stesso (tutore/curatore/ amministratore di sostegno: si rimanda al riguardo alle "*Regole in materia di operazioni con persone fisiche*") - può esercitare i diritti riconosciuti dal Regolamento riportati al cap. 3.2 del presente documento.

Si precisa che la richiesta può essere formulata:

- in forma libera, o mediante apposito modulo di esercizio dei diritti reperibile sul sito web della Banca o richiedibile al Gestore in filiale, completa degli estremi identificativi del documento di riconoscimento, allegato in copia, dell'Interessato, datata e sottoscritta. La richiesta presentata da soggetto diverso dall'Interessato deve essere corredata da copia del mandato conferito dall'Interessato a tale soggetto, debitamente firmato, o dell'atto di nomina a tutore/curatore/amministratore di sostegno e relativo atto di giuramento (cfr. Regole cit. sopra). Tutta la documentazione deve essere conservata nella posizione del cliente. Se la documentazione non è completa, viene richiesto all'Interessato di integrare la stessa al fine di poter evadere la richiesta;

- tramite i canali disponibili (direttamente in filiale, posta, mail, online). Nel caso di richieste pervenute direttamente in filiale, effettuate sia in forma scritta che in forma orale, deve essere richiesta l'esibizione del documento di riconoscimento a comprova della titolarità del diritto; per le richieste pervenute sulla pagina social della Banca (ad es. Facebook Twitter, LinkedIn, etc.), la funzione deputata a moderarne i contenuti (es. Gestore della Filiale Online), in base al tipo di richiesta, indirizza la clientela verso altri canali di gestione (filiale/Internet Banking) o altrimenti fornisce al richiedente i dati di contatto del Data Protection Officer a cui rivolgere la richiesta.

L'Autorizzato che acquisisce la richiesta provvede, in caso di richiesta scritta, ad apporre il timbro attestante la data di ricezione o, in caso di richiesta orale, a registrare la richiesta inviando una e-mail tramite la propria casella di struttura alla casella mail privacy@intesasanpaolo.com indicando i dati identificativi del richiedente e una descrizione della richiesta. In caso di richiesta scritta, la trasmette in

---

([24]) Ove necessaria, tale segnalazione sarà disposta conformemente al *Provvedimento sulla notifica delle violazioni dei dati personali (data breach) del 30 luglio 2019*.

originale al Data Protection Officer anticipandola comunque via e-mail tramite la propria casella di struttura alla casella mail privacy@intesasanpaolo.com[25].

L'Autorizzato operante in filiale evade direttamente la richiesta solo quando la stessa concerne:

- esercizio del diritto di rettifica e/o integrazione dei dati: se la richiesta è pervenuta al Gestore e/o all'Assistente, questi evadono direttamente e senza ingiustificato ritardo le richieste di aggiornamento, rettifica o integrazione. Le relative attività (es. variazione indirizzo postale, inserimento/variazione recapito telefonico, inserimento/variazione recapito elettronico) sono effettuate con le consuete modalità operative utilizzando i sistemi informativi a supporto;

- revoca del consenso: se la richiesta è pervenuta al Gestore e/o all'Assistente questi evadono direttamente e senza ingiustificato ritardo le richieste di modifica del consenso con le consuete modalità operative utilizzando i sistemi informativi a supporto. Si veda cap. 4.3.2 del presente documento.

Con riferimento alle richieste di accesso degli interessati all'elenco dei soggetti individuati come Titolari, Responsabili o Contitolari del trattamento dati personali si rappresenta che tale elenco, come indicato nell'**informativa nei confronti di persone fisiche ai sensi dell'art. 13 e 14 del Regolamento (UE) 2016/679**, deve essere sempre accessibile ovvero consultabile per gli Interessati presso tutte le Filiali. Il Gestore di filiale può reperire la copia aggiornata di tale elenco in ARCO nella Sezione: Documentazione-Modulistica-Compliance_e_Adempimenti_ di_ Legge-Tutela _Aziendale – Privacy.

Tutte le istanze di un cliente, diverse da una di quelle sopra citate o contenenti il riferimento al "GDPR" o parole quali "Autorità Garante", "Privacy", "trattamento dati personali", "*data breach*" pervenute ad una filiale o ad altra funzione aziendale (ad esempio alla Gestione Reclami), devono essere tempestivamente trasmesse al DPO, per le valutazioni di merito, in proposito si veda quanto previsto nella "*Guida di Processo Gestione della Conformità – Gestione ambito normativo Tutela della privacy*".

Qualora dalla richiesta non sia possibile accertare l'identità dell'Interessato, il Data Protection Officer provvede a richiedere le evidenze necessarie (a seconda dei canali utilizzati, esibizione o invio di una copia di un documento d'identità in corso di validità). In questo caso, i tempi per la risposta decorrono dal momento del ricevimento della documentazione integrativa ai fini dell'accertamento di identità.

([25]) Agli interessati sono invece indicati nelle informative quali recapiti ufficiali di posta elettronica per l'esercizio dei diritti dpo@intesasanpaolo.com e/o privacy@pec.intesasanpaolo.com.

4.10 Trattamento di dati per scopi di marketing

In considerazione dei numerosi interventi del Garante in tema di uso di dati personali a scopo di marketing e pubblicità, nonché della specifica regolamentazione dell'attività di marketing nei confronti di persone giuridiche, enti o associazioni, si evidenziano di seguito, per le principali fonti di dati personali, le relative misure da adottare per consentire lo svolgimento dell'attività di marketing in conformità al modello di accountability individuato, fermo restando che ogni specifico e ulteriore indirizzamento va determinato nell'ambito del processo di Privacy by Design dell'iniziativa (come previsto anche nell'ambito "*Linee Guida per l'approvazione di nuovi prodotti, servizi e attività destinati a un determinato target di clientela*").

Si precisa, inoltre, che gli eventuali consensi commerciali, utili per attivare trattamenti funzionali alle attività di marketing della Banca e del Gruppo rilasciati dall'Interessato, decadono con la chiusura di tutti i rapporti che l'Interessato ha in essere con la Banca.

4.10.1 Utilizzo di banche dati interne

L'utilizzo a scopo di marketing di dati personali afferenti persone fisiche, presenti nelle banche dati interne è consentito solo in merito ai clienti (continuativi, occasionali o potenziali) che abbiano manifestato lo specifico consenso.

Pertanto, al cliente a cui sia già stato venduto un prodotto o prestato un servizio è possibile proporre analogo prodotto o servizio, a meno che questi non abbia espressamente negato il consenso a tali iniziative o abbia omesso di esprimerlo.

Più in generale, si evidenzia che **la creazione di nuove banche dati interne deve essere preventivamente concordata con il DPO** nell'ambito del processo di Privacy by Design.

4.10.2 Acquisizione di dati da società terze/banche dati esterne

L'acquisizione di dati personali riferiti a persone fisiche da società terze (per esempio: banche dati offerte da società specializzate, elenchi di nominativi di studenti forniti dalle scuole, elenchi forniti da Associazioni di categoria/Albi professionali), indipendentemente dal loro formato e dalla numerosità di cui si compone la banca dati medesima, è consentita a fronte dell'adozione di alcune cautele da parte di chi sottoscrive il contratto con la società terza e specificamente:

- presenza nel contratto di precise clausole che precisino che tutti i soggetti inseriti nella lista/banca dati abbiano ricevuto l'adeguata Informativa e rilasciato lo specifico consenso alla comunicazione dei propri dati personali a terzi e al loro uso a fini commerciali anche in relazione all'attività di marketing telefonico e postale o all'uso di sistemi automatizzati (fax, e-mail, sms, chiamate senza operatore), manlevando la Banca da ogni responsabilità in merito,

- previsione contrattuale di poter verificare la modulistica utilizzata sia come Informativa sia per la raccolta del consenso, oltre alla possibilità di poter verificare a campione l'evidenza del consenso rilasciata dal singolo Interessato.

Si rammenta, inoltre, che non è consentito l'utilizzo dei dati personali presenti sulle banche dati relative ai Sistemi di Informazioni Creditizie "SIC" per scopi di marketing.

4.10.3 Acquisizione di dati da elenchi o registri pubblici

Per quanto riguarda gli elenchi pubblici, occorre osservare che la finalità della presenza di dati personali riferiti a persone fisiche in detti elenchi non è quella di ricevere promozioni commerciali; pertanto, in caso di contatto con soggetti appartenenti a dette liste, occorre raccogliere preventivamente uno specifico consenso per finalità di marketing e fornire idonea Informativa.

4.10.4 Utilizzo di dati da elenchi degli abbonati ai servizi di telefonia

La regolamentazione del marketing telefonico e cartaceo disposta con il D.P.R. n. 178/2010 e successive modificazioni, per cui i "contraenti" possono opporsi all'utilizzo per finalità pubblicitarie dei propri dati personali presenti negli elenchi telefonici, relativi ai numeri pubblici di cui si è intestatari e ai corrispondenti indirizzi postali associati, nonché la Legge n. 5/2018 con riferimento all'estensione del diritto di opposizione al marketing telefonico a tutti i numeri riservati, inclusi i cellulari, stabiliscono che le attività di telemarketing e marketing postale sono realizzabili nei confronti delle persone fisiche, giuridiche, enti o associazioni che non risultino presenti (c.d. "iscritti") nel Registro delle Opposizioni.

Pertanto, in conformità alle citate disposizioni, le società che intendono contattare gli "utenti" per attività commerciali, promozionali o per il compimento di ricerche di mercato tramite l'uso del telefono, sono tenute a registrarsi al sistema gestito dalla Fondazione Ugo Bordoni - gestore del servizio – e a comunicare la lista dei numeri che intendono contattare. Il gestore, mettendo a confronto le informazioni contenute nel Registro delle Opposizioni e la lista dei numeri fornita dalla società, eliminerà da quest'ultima i numeri degli "utenti" che abbiano fatto richiesta di non essere contattati. La lista aggiornata dal gestore, ovvero "filtrata", ha validità quindicinale.

Attualmente l'opposizione al telemarketing e marketing postale non annulla la validità dei consensi per contatti con finalità commerciali rilasciati direttamente dagli utenti alle singole società (per esempio in occasione della stipula dei contratti, adesione alle iniziative destinate alla clientela *prospect*).

Inoltre, nei riguardi delle persone giuridiche, enti o associazioni, le comunicazioni possono essere effettuate tramite posta elettronica, telefax, SMS, MMS e altri sistemi elettronici automatizzati o tramite telefono senza intervento dell'operatore solo se l'Interessato ha espresso il proprio consenso a tali iniziative.

4.10.5 Utilizzo di dati acquisiti da Internet

In mancanza di un preventivo consenso dell'Interessato, non è lecito l'utilizzo per finalità di marketing di:

- dati relativi a persone fisiche pubblicati su un sito o pagina web per scopi di informazione aziendale, istituzionale o associativa;
- liste di abbonati a provider;
- dati ricavabili da forum on-line e newsgroup o l'indirizzo IP (Internet Protocol)[26] di un device.

4.10.6 Utilizzo di dati da Profilazione

La profilazione consiste nella raccolta di informazioni relative ad un Interessato (o un gruppo di Interessati) e nella successiva valutazione delle loro caratteristiche o dei loro modelli di comportamento, al fine di includerli in una determinata categoria o gruppo, per analizzare e/o fare previsioni, ad esempio, in merito a:

- capacità di eseguire un compito;
- interessi;
- comportamento d'acquisto probabile.

Il Regolamento introduce disposizioni per garantire che la profilazione e il processo decisionale automatizzato relativo alle persone fisiche non siano utilizzati in maniera tale da avere un impatto ingiustificato sui diritti delle persone. Esso prevede, ad esempio:

- requisiti specifici di trasparenza e correttezza;
- maggiori obblighi in termini di responsabilizzazione;
- basi giuridiche specifiche per il trattamento;
- il **diritto delle persone fisiche di opporsi alla profilazione, segnatamente alla profilazione per finalità di marketing**;
- qualora siano soddisfatte determinate condizioni, la necessità di effettuare una valutazione d'impatto in termini privacy.

Pertanto, qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo dei medesimi per valutare determinati aspetti relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica, con l'obiettivo di offrire promozioni commerciali mirate, è consentita solo in

---

([26]) L'indirizzo IP (Internet Protocol) è un codice numerico che identifica ogni singolo device connesso ad una rete, è considerato un dato personale (in tal senso si è pronunciata anche la Corte di Giustizia Europea Causa C-582/14 "*Patrick Breyer*" contro "*Bundesrepublik Deutschland*" sentenza della seconda Sezione del 19 ottobre 2016).

merito a Interessati, quali clienti continuativi, occasionali o potenziali, che abbiano manifestato lo specifico consenso.

4.10.6.1 Utilizzo di cookie e altri strumenti di profilazione online

I siti web e le applicazioni accessibili/fruibili via Web delle Società del Gruppo possono fare utilizzo di cookie e di altri strumenti di identificazione dell'utente per finalità di profilazione e marketing; è anche possibile la presenza di cookie e di altri strumenti "di terze parti" per tracciare le attività dell'utente e mostrare annunci pubblicitari coerenti con il comportamento di navigazione.

Tali trattamenti devono essere preceduti da un'Informativa specifica, secondo le modalità prescritte e subordinati all'acquisizione del consenso dell'Interessato che dovrà essere raccolto e documentato secondo le previsioni del Regolamento (si veda cap. 4.3.1 del presente documento). Risulta, pertanto, non conforme e vietata[27] la pratica di installazione dei cookie mediante caselle di spunta preselezionate o l'implementazione di cookie wall[28], mentre si evidenzia come è necessario informare l'utente, al momento in cui gli è chiesto di prestare il proprio consenso all'uso dei cookie di profilazione, del periodo di attività degli stessi e se presenti cookie di terza parte.

Quindi, ogni qualvolta venga realizzato un nuovo sito internet, anche per il tramite di fornitori, o si attivino campagne di "advertising online", è necessario coinvolgere il DPO nell'ambito del Processo di Privacy by Design, per la valutazione di eventuali necessità di adeguamenti informatici.

4.11 Trattamento di dati nell'ambito dei sistemi di videosorveglianza e controllo accessi biometrico

Con riferimento ai dati personali trattati dalla Banca nell'ambito delle attività di videosorveglianza, ovvero quali quelli acquisiti e trattati con impianti di videosorveglianza remota, videoregistrazione, impianti biometrici di rilevazione delle impronte digitali associata a videoregistrazione delle immagini e sistemi di controllo accessi biometrici ad aree riservate dei Palazzi, si specifica che questi trattamenti sono finalizzati unicamente alla tutela della sicurezza del patrimonio aziendale ed alla prevenzione dei reati e non è pertanto diretto ad attività di controllo a distanza dei lavoratori e/o di schedatura degli interessati[29].

([27]) In tal senso si è pronunciata anche la Corte di Giustizia Europea Causa C-673/17 "*Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*" contro "Planet49 GmbH" in data 1° ottobre 2019.

([28]) Pratica che condiziona l'accesso ad un sito web sino a quando l'interessato non accetti i cookie del caso o proceda, mediante le apposite impostazioni, alla scelta tra i cookie installati.

([29]) A tal riguardo si evidenzia che, oltre alla disciplina di protezione dei dati, deve essere rispettata anche la normativa in materia di controllo a distanza dei lavoratori, di cui all'art. 4. della Legge n. 300/1970 (c.d. "Statuto dei lavoratori"), che subordina l'installazione di impianti di videosorveglianza alla sottoscrizione con di accordo

Ferma restando l'applicabilità dei principi e delle ordinarie garanzie poste dal GDPR (quali Privacy by design e by default) anche ai trattamenti in oggetto, nel seguito si evidenziano le principali misure da adottare per consentire la conformità di questo trattamento in virtù del Regolamento, delle Linee Guida EDPB 3/2019 "on processing of personal data through video devices" del 29 gennaio 2020 e del *Provvedimento del Garante in materia di videosorveglianza dell'8 aprile 2010*.

4.11.1 Autorizzato al trattamento nei sistemi di video sorveglianza e biometrici di vigilanza

Conformemente a quanto illustrato nel cap. 4.1 del presente documento, sono opportunamente individuati come soggetti **Autorizzati al trattamento dei dati relativi alla videosorveglianza: le Guardie Particolari Giurate** operanti presso la Control Room di Intesa Sanpaolo, in quanto collaboratori dell'azienda e dipendenti di un Istituto di Vigilanza con il ruolo soggettivo di Responsabile del Trattamento, il **Direttore della Filiale** o, per un Palazzo, il **dipendente preposto** specificatamente individuato.

Le **Guardie Particolari Giurate** operanti presso la Control Room di Intesa Sanpaolo nell'ambito di tale autorizzazione assumono la responsabilità:

- dell'**attuazione della videosorveglianza remota degli ambienti delle Filiali e dei Palazzi**. Per il solo ambito delle Filiali le Guardie Particolari Giurate possono anche inviare messaggi vocali (cosiddetta Guardia virtuale). Il sistema registra solo presso le Filiali e i Palazzi le immagini, sui sistemi di videoregistrazione digitale ivi esistenti;

- della **verifica del funzionamento dei sistemi**, con l'ausilio del personale dipendete di Intesa Sanpaolo. Controllano inoltre che le telecamere siano correttamente orientate, in base alle attività di videosorveglianza remota che il sistema deve garantire, e che data e ora del sistema siano corrette;

- di **richiedere l'intervento dei manutentori in caso di guasto** o necessità di riposizionamento telecamere, con l'ausilio del personale dipendete di Intesa Sanpaolo, e verificare l'esito dell'intervento stesso.

Il Direttore della Filiale o, per un Palazzo, il dipendente preposto specificatamente individuato ,nell'ambito di tale autorizzazione assume la responsabilità:

- della **gestione delle chiavi** dell'armadio contenente l'apparato di videoregistrazione;

---

collettivo con le rappresentanze sindacali. In mancanza di accordo, gli impianti di videosorveglianza possono essere installati "previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro".

- della corretta **conservazione di eventuali password** per l'accesso ai dati[30];
- della **verifica periodica degli impianti**, almeno mensile per gli impianti di tipo analogico, semestrale per quelli di tipo digitale, in termini di: i) apparato funzionante - led accesi -, ii) effettiva registrazione delle immagini riprese dalle telecamere, ove la tecnologia e il tipo dell'impianto lo consenta, iii) qualità delle immagini[31], iv) corretto orientamento delle telecamere, per cui devono essere ripresi l'ingresso principale della Filiale e la zona riservata al pubblico, con esclusione quindi delle zone uffici, salvo i casi espressamente previsti, v) correttezza della data e dell'ora memorizzate nella registrazione;
- di **richiedere l'intervento** dei servizi di manutenzione **in caso di guasti o anomalie**;
- di **curare l'esposizione** ed il mantenimento dei **cartelli informativi** per gli Interessati;
- con riferimento alle sole Filiali dotate di un dispositivo biometrico, dovrà conservare come documentazione specifica[32] a disposizione di eventuali controlli da parte del Garante:
    - il documento da cui si evincano le condizioni di rischio della Filiale e della metodologia di valutazione del medesimo;
    - la documentazione tecnica del dispositivo biometrico adottato;
    - il particolare della planimetria della Filiale (o, in alternativa, planimetria di una Filiale "tipo") con riporto dei componenti principali del sistema;
    - la copia dell'informativa "interna" alla clientela e la copia dell'informativa "esterna" alla clientela;
    - lo stralcio della normativa relativa alle modalità alternative di accesso della clientela;
    - inoltre, avrà cura di comunicare anche ad un suo delegato il luogo di custodia della citata documentazione che dovrà essere prontamente messa a disposizione in caso di controlli.

Per gli impianti di rilevazione delle impronte digitali associata a videoregistrazione delle immagini vi è quale **Autorizzato al trattamento dei dati biometrici**, la figura del "**Vigilatore dei Dati**". Questi o un soggetto parimenti indipendente da lui designato, è l'unico che può venire lecitamente a conoscenza dei dati personali acquisiti dai sistemi biometrici di vigilanza.

([30]) Le chiavi, per le sole Filiali, sono gestite in analogia a quelle dei mezzi forti di Filiale utilizzando il Registro Chiavi dei Mezzi Forti, come previsto dalle "*Regole di Sicurezza Fisica per le Reti Territoriali della Banca*".

([31]) Le verifiche in merito alla qualità delle immagini registrate dovranno essere eseguite a cura dell'Autorizzato anche in occasione di visite manutentive, nel corso delle quali dovranno essere effettuate, per tutte le tipologie di impianti, le verifiche descritte.

([32]) Per richieste afferenti i documenti della ex-verifica preliminare fare riferimento alla Struttura Direzione Centrale Tutela Aziendale.

Il Vigilatore dei Dati sovraintendendo all'intero processo crittografico dei dati biometrici, ha il compito di impartire le istruzioni necessarie e garantire:

- l'interposizione tra le filiali stesse ed i richiedenti di accesso "in chiaro", sia per esigenze di giustizia sia in caso di esercizio dei diritti dell'interessato;
- l'aggiornamento trimestrale delle password;
- l'aggiornamento del registro delle chiavi di accesso della Filiale;
- lo stoccaggio in apposito deposito delle chiavi e delle password di accesso ai sistemi di crittografia.

Per i sistemi di controllo accessi biometrici, utilizzati per l'accesso ad aree riservate dei Palazzi, un soggetto esterno collaboratore dell'azienda o un dipendente di Intesa Sanpaolo, opererà come **Autorizzato al trattamento dei dati biometrici** con il compito di sovrintendere:

- all'acquisizione di un template delle impronte digitali dell'interessato;
- all'emissione di un badge contente il template stesso;
- alla consegna del badge all'interessato.

Si precisa che il template delle impronte deve essere:

- acquisito solo dopo aver reso specifica informativa e acquisito l'autorizzazione al trattamento da parte dell'interessato (i template biometrici di persone non consenzienti non vengano acquisiti);
- prodotto senza alcuna capacità retroattiva di recuperare i dati personali che l'impronta conteneva in precedenza;
- memorizzato esclusivamente sul tesserino aziendale in possesso dell'interessato.

Riguardo quest'ultimo punto la fase di acquisizione dell'impronta, con la sola finalità di generare il template (c.d. "enrollment"), deve prevede che una volta ottenuto il risultato tutti i modelli intermedi vengano immediatamente e irreversibilmente cancellati: è pertanto esclusa la loro memorizzazione o archiviazione.

4.11.2 Informativa specifica agli interessati

Posto che alla base delle attività di trattamento dei sistemi di *videosorveglianza remota, videoregistrazione e impianti biometrici di rilevazione delle impronte digitali associata a videoregistrazione delle immagini Palazzi*, vi sia il legittimo interesse della Banca, i soggetti che entreranno nel raggio di azione di detti dispositivi devono essere comunque informati con apposita informativa, anche di tipo sintetico, esposta in modo da essere **visibile prima** di venire compromessi **dal campo di ripresa** delle telecamere ovvero prima che i **dati siano rilevati** e quindi:

- prima dell'accesso, anche ai varchi a doppia porta o bussole, con apposito avviso (c.d. "informativa esterna" o "di primo livello");

- internamente ai locali della Filiale o del Palazzo con apposita informativa (c.d. "informativa interna" o "di secondo livello") in cui si indica il Titolare dei trattamenti, le finalità e modalità di trattamento, i soggetti che sono legittimati alla visione ed i riferimenti per l'esercizio dei diritti.

L'esposizione ed il mantenimento degli avvisi e delle informative[33] sono a cura del Personale individuato come ***Autorizzato al trattamento dei dati relativi alla video sorveglianza*** presso Filiali e Palazzi.

Per i sistemi di videosorveglianza, visto l'interesse legittimo e il compito di interesse pubblico svolto dalla Banca, anche in presenza di un diritto d'opposizione da parte di un soggetto non sussistono validi motivi per interrompere l'elaborazione dei dati personali da parte della telecamere.

Viceversa, come prescritto dall'Autorità Garante e dall'EDPB, l'Interessato che segnalasse il proprio **rifiuto di sottoporsi alla lettura dell'impronta digitale** deve essere fatto accedere in Filiale escludendo il funzionamento del rilevatore biometrico ed adottando, ove ritenuto necessario, misure cautelative (ad es.: richiesta di esibizione di un documento di riconoscimento); in questi casi non si deve comunque tenere un comportamento vessatorio. Analogo comportamento deve essere tenuto per gli accessi ai locali di sede centrale o altri locali aperti al pubblico da parte dei soggetti preposti.

Inoltre, per quanto ovvio, si segnala che il Personale non è tenuto ad utilizzare il sistema di lettura dell'impronta digitale per accedere in Filiale.

Infine, per i sistemi di controllo accessi biometrici utilizzati per l'accesso ad aree riservate dei Palazzi, l'informativa è resa prima dell'acquisizione del template biometrico, insieme alla contestuale raccolta del consenso esplicito al trattamento dei dati personali. L'interessato può, in ogni momento, modificare le proprie espressioni di consenso, decidendo di conferire un consenso prima negato, o di revocarne uno dato.

4.11.3 Le istanze di accesso ai dati: Autorità Giudiziaria o di Polizia e Interessati

In relazione al compimento di atti delittuosi, o per motivi connessi allo svolgimento di indagini, la **Magistratura e la Polizia Giudiziaria** possono richiedere la consegna delle immagini acquisite dai sistemi di videosorveglianza e, ove presenti gli appositi sistemi, delle impronte in chiaro e delle immagini associate al transito.

In tali circostanze, l'**Autorizzato al trattamento dei dati relativi alla video sorveglianza** avrà cura di:

- **richiedere** all'Autorità Giudiziaria o di Polizia il rilascio di **apposito verbale** di sequestro o di acquisizione che riporti data e, se possibile, orario indicativo di interesse. Ciò, allo scopo di

[33] Tali informative (c.d. "interna" e c.d. "esterna") sono reperibili in ARCO alla Sezione: Modulistica/Compliance e Adempimenti di Legge/Tutela Aziendale – Privacy.

valutare preliminarmente la presenza dei dati, in ragione del limite massimo di conservazione di 7 giorni solari;

- **informare tempestivamente**, se presenti gli specifici sistemi, la figura del "**Vigilatore dei Dati**" quale **Autorizzato al trattamento dei dati biometrici** per l'intervento di decriptazione delle informazioni riferite alle impronte ed alle immagini dello specifico sistema. Come specificatamente indicato nelle informative per la clientela, le impronte e/o le immagini registrate sono crittografate e non possono essere visualizzarle in alcun modo dal Personale delle Filiali.

In riferimento alle **richieste di accesso** ai dati, quali le immagini acquisite dai sistemi di videosorveglianza e, ove presenti, delle impronte digitali e delle immagini associate al transito, effettuate **dai soggetti Interessati** allo specifico trattamento, posto che l'informativa affissa indica tutte le informazioni necessarie per esercitare questo e i restanti diritti[34] riconosciuti dal Regolamento, si segnala che queste vanno gestite come indicato al cap. 4.9 del presente documento, e, parallelamente, di allertare sia il "**Vigilatore dei Dati"**, quale **Autorizzato al trattamento dei dati biometrici** per l'intervento di decriptazione delle informazioni riferite alle impronte ed alle immagini dello specifico sistema sia l'**Autorizzato al trattamento dei dati relativi alla videosorveglianza**. Posto che deve essere fatta particolare attenzione affinché **non vengano mostrate immagini non di pertinenza dell'Interessato**, precauzione che deriva sia dall'obbligo di non comunicare o rendere accessibili a terzi dati personali a loro non afferenti sia da evidenti esigenze di sicurezza, l'**Autorizzato al trattamento dei dati relativi alla videosorveglianza** così come l'**Autorizzato al trattamento dei dati biometrici** (c.d. "Vigilatore dei dati") dovrà preventivamente esaminare in via separata tutte le immagini ove compare l'Interessato, al fine di decidere quali possano essere mostrate ovvero quali immagini possano essere visionate dall'interessato stesso, solo previo **appropriato oscuramento** di tutti gli altri eventuali soggetti non pertinenti. A seguito di tali attività, da effettuarsi entro un mese dalla richiesta affinché siano garantito il rispetto di quanto previsto dal Regolamento per il riscontro, il DPO fornirà risposta scritta all'Interessato.

Nel caso, infine, in cui pervengano le richieste di accesso ai dati, tanto da parte dell'Interessato, quanto dell'Autorità Giudiziaria o di Polizia, riferite a periodi concomitanti, o, più in generale ad uno stesso evento delittuoso, si darà priorità alla richiesta proveniente dall'Autorità Giudiziaria o di Polizia, indipendentemente dalla data di inoltro della stessa. Per contro, l'istanza di accesso ai dati da parte dell'Interessato non potrà essere accolta senza il preventivo parere favorevole della medesima Autorità Giudiziaria o di Polizia titolare delle indagini.

Più in generale, resta fermo che l'**Autorizzato al trattamento dei dati relativi alla videosorveglianza** così come l'**Autorizzato al trattamento dei dati biometrici**, **in presenza di una richiesta di accesso**

([34]) Con riferimento al diritto di opposizione e cancellazione avanzata dall'Interessato, fermo restando il diritto di cancellazione in caso di illecito, si rappresenta che il Titolare si vedrà costretto a respingere detta istanza giacché prevalente il legittimo interesse del Titolare a proteggere l'incolumità degli individui e a prevenire i reati.

da parte dell'Interessato oppure di eventi criminosi verificatisi o, ancora, di una richiesta da parte dell'Autorità Giudiziaria o di Polizia, **potrà assicurare la disponibilità dei dati raccolti**, salvando su supporti removibili le informazioni d'interesse o conservando la specifica videocassetta, evitando, in tal modo, la cancellazione automatica o manuale alla scadenza del periodo di conservazione previsto pari a sette giorni. Nelle sopradette circostanze l'Autorizzato, una volta in possesso delle informazioni utili ad individuare con esattezza l'evento - in primis la data e l'intervallo orario - procederà alla conservazione della videocassetta relativa al periodo (per sistemi analogici) o all'estrazione dei dati ed al successivo salvataggio su supporto removibile con l'eventuale ausilio dei tecnici manutentori. Il citato supporto dovrà essere **custodito in plico chiuso sigillato controfirmato** dallo stesso Autorizzato e da un altro collega all'uopo[35] individuato, per il conseguente deposito all'interno di un mezzo di custodia in uso secondo lo schema:

- nei casi di eventi delittuosi o di istanza da parte dell'Autorità Giudiziaria o di Polizia, i dati saranno conservati fino alla consegna alla stessa previo ritiro di verbale di sequestro o di acquisizione;
- in caso di istanza da parte dell'Interessato, i dati salvati saranno tenuti a disposizione per 30 giorni, trascorsi i quali il plico in questione sarà distrutto direttamente dall'Autorizzato previa redazione di apposito verbale da allegare al registro delle chiavi.

Per i sistemi videosorveglianza remota e di controllo accessi biometrici utilizzati per l'accesso ad aree riservate dei Palazzi si precisa che, non essendo prevista alcuna registrazione di dati personali per immagini o per dati biometrici, non è applicabile alcuno iter di accesso agli stessi.

4.12 Sanzioni

Tutti gli Autorizzati sono tenuti ad osservare e a far osservare le disposizioni contenute nelle presenti Regole per il trattamento e la protezione dei dati personali.

Nel rispetto dei diritti e delle libertà fondamentali degli Interessati, dei principi di pertinenza e non eccedenza previsti dal Regolamento, nonché delle presenti Regole di trattamento dei dati personali, la Banca potrà effettuare verifiche per rilevare eventuali comportamenti anomali con la finalità di tutelare gli interessi aziendali.

Il mancato rispetto o la violazione delle suddette Regole può determinare: i) per il personale dipendente, l'adozione dei **provvedimenti di natura disciplinare** previsti dal Contratto Collettivo Nazionale di Lavoro tempo per tempo vigente, nonché le **azioni civili e penali stabilite dalla legge**, ii) per i collaboratori esterni, la risoluzione del contratto e l'eventuale risarcimento del danno, ferme restando le eventuali azioni penali stabilite dalla legge.

([35]) Per l'Autorizzato al trattamento dei dati biometrici (c.d. "Vigilatore dei dati") la seconda firma sarà quella dell'Autorizzato al trattamento dei dati relativi alla video sorveglianza.

5 Appendice

Di seguito si riporta una prima collezione di riferimento della normativa a livello nazionale ed europeo. Mentre per una prima consultazione della normativa di riferimento extra UE in materia di trattamento dati personali, è possibile riferirsi al documento di Legal Inventory[36], prodotto della Direzione Centrale Tutela Aziendale.

Tra le Linee Guida e Provvedimenti del Garante Privacy si segnalano in particolare:

- Linee Guida per la posta elettronica e internet, adottate con Provvedimento n.13 del 1° marzo 2007
- Linee Guida per trattamenti dati relativi al rapporto banca-clientela n.53 del 25 ottobre 2007
- Linee Guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati n.53 del 23 novembre 2006
- Linee Guida in materia di riconoscimento biometrico e firma grafometrica n.513 del 12 novembre 2014
- Linee Guida in materia di trattamento di dati personali per profilazione on line n.161 del 19 marzo 2015
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (*Data Breach*) – n.157 del 30 luglio 2019
- Provvedimento del Garante sul trattamento di categorie particolari di dati n.176 del 29 luglio 2019
- Provvedimento del Garante sul trattamento dei dati personali relativi ad un conto bancario n.286 del 22 giugno 2017
- Provvedimento in materia di informativa e acquisizione del consenso per l'uso dei cookie n.229 dell´8 maggio 2014
- Provvedimento generale prescrittivo in tema di biometria n.513 del 12 novembre 2014
- Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie – n.192 del 12 maggio 2011

([36]) Il documento è disponibile nella Intranet aziendale alla Sezione Privacy tramite il percorso: Gruppo – Governance – Strutture a diretto riporto dei Vertici Aziendali – Tutela Aziendale – Privacy - Legal Inventory, i suoi contenuti sono organizzati per gli ambiti di:

1. Data Categories;
2. Data Processing;
3. Data Transfer;
4. Data Security;
5. Data Breach;
6. Roles and Responsibilities;
7. Banking Secrecy;
8. Labor Law.

- 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 n.16 del 19 gennaio 2011
- Provvedimento in materia di videosorveglianza n.99 dell'8 aprile 2010
- Modifiche del Provvedimento n.300 del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento n.149 del 25 giugno 2009
- Rilevazione di impronte digitali ed immagini per accedere agli istituti di credito del 27 ottobre 2005
- Provvedimento in materia di protezione dei dati personali - Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti n.163 del 12 settembre 2019

Tra i documenti di maggior rilievo dell'European Data Protection Board:

- Guidelines 05/2020 on consent under Regulation 2016/679 – version 1.1 adopted on 4 May 2020
- Guidelines 3/2019 on processing of personal data through video devices - version 2.0 adopted on 29 January 2020 after public consultation
- Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725)
- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version for public consultation
- EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation
- EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - version adopted after public consultation
- EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version for public consultation
- EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation

L'European Data Protection Board ha inoltre recepito i seguenti documenti del WP29:

- Guidelines on transparency under Regulation 2016/679, WP260 rev.01
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01
- Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01
- Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01
- Guidelines on Data Protection Officers ('DPO'), WP243 rev.01

- Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01
- Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR
- Working Document Setting Forth a Co-Operation Procedure for the approval of Binding Corporate Rules for controllers and processors under the GDPR, WP 263 rev.01
- Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264
- Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265
- Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01
- Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01