Banca di Credito Cooperativo di Bari Soc. Coop.

"Politica per la protezione dei dati personali"

delibera del CdA del 27.06.2018

INDICE

1. OGGETTO

La presente Politica definisce i principi generali, il modello organizzativo, i principali ruoli e le responsabilità finalizzati a tutelare, nell'ambito dei trattamenti effettuati dalla Banca o dei quali essa assuma responsabilità, il diritto alla protezione dei dati personali in coerenza con le prescrizioni normative vigenti.

Il contenuto della Politica tiene in considerazione l'evoluzione normativa in materia, principalmente costituita dall'adozione del "Regolamento Europeo per la Protezione dei Dati" (di seguito anche "Regolamento" o "GDPR").

2. AMBITO DI APPLICABILITA', APPLICAZIONE, AGGIORNAMENTO

La presente Politica è approvata dal Consiglio di Amministrazione della Banca. Ogni modifica alla stessa segue il medesimo iter approvativo.

La presente Politica ed i suoi aggiornamenti verranno resi noti alle terze parti individuate come "Responsabili di trattamento" (di seguito anche "Responsabile") tramite la pubblicazione sul sito internet.

3. PRINCIPALI RIFERIMENTI NORMATIVI

Banca d'Italia – "Disposizioni di vigilanza per le banche", Circ. 285 del 17 dicembre 2013 e successivi aggiornamenti;

Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio (Regolamento generale sulla protezione dei dati).

Provvedimento dall'Autorità Garante per la Protezione dei Dati Personali del 27 novembre 2008 - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema.

Oltre alle fonti normative indicate, i processi collegati alla presente Politica devono tenere in considerazione l'insieme normativo di riferimento applicabile (Regolamenti Europei, Legislazione Nazionale, Provvedimenti, Autorizzazioni nonché Linee Guida dell'Autorità Garante per la Protezione dei Dati Personali).

4. DEFINIZIONI

Ai fini della presente politica e delle relative norme di processo sono rilevanti le seguenti definizioni tratte dal "Regolamento":

1. «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;
2. «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la

comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3. «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4. «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5. «pseudonimizzazione»:il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6. «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7. «titolare del trattamento» o «Titolare»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8. «responsabile del trattamento» o «Responsabile»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9. «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. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
10. «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;
11. «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 inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
12. «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13. «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;
14. «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;
15. «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;
16. «trattamento transfrontaliero»: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

Inoltre, ai fini della presente politica e delle relative norme di processo, s'intende per:

- «dati sensibili»: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati personali relativi a condanne penali e ai reati;
- «Contitolare»: il Titolare di trattamento di dati personali che ne determina le finalità e i mezzi congiuntamente alla Banca;
- «Interessato»: la persona fisica i cui dati personali sono oggetto di trattamento;
- «Referente del Trattamento»: il responsabile di unità organizzativa o Ruolo Funzionale che sia primariamente responsabile di un trattamento di dati personali e che abbia ricevuto una connessa designazione;
- «incaricato al trattamento» (o «Incaricato»): la persona fisica autorizzata dalla Banca allo svolgimento di attività nell'ambito di un trattamento di dati personali svolto internamente;
- «incaricato esterno al trattamento» (o «incaricato esterno»): l'incaricato al trattamento non legato alla Banca da rapporto di lavoro dipendente;
- «amministratore di sistema»: figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di suoi componenti, tra cui gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

5. DISPOSIZIONI DI CARATTERE GENERALE

Nello svolgimento delle proprie attività, la Banca (sia che operi in qualità di "Titolare" che di "Responsabile") adotta specifiche e puntuali misure per assicurare che il trattamento dei dati personali avvenga in conformità ai requisiti normativi, alle istruzioni fornite, e ove applicabile ricevute dal "Titolare", e seguendo le migliori pratiche, al fine di tutelare i diritti

degli interessati, minimizzare i rischi connessi ai trattamenti e garantendo la dimostrabilità delle misure adottate.

5.1 Gestione dei trattamenti di dati personali

La Banca predispone e mantiene aggiornato un “Registro delle attività di trattamento” svolti in qualità di Titolare o di Responsabile; il Registro deve contenere come minimo le informazioni ed i dati per esso previsti dalla applicabile normativa comunitaria e nazionale e le modalità di aggiornamento e conservazione sono formalmente descritte ed assegnate.

Per ogni trattamento è identificata la struttura che ne è primariamente responsabile ed il Referente del Trattamento (di norma, il Responsabile di tale struttura).

Il Registro contiene almeno le seguenti informazioni di carattere generale per i trattamenti svolti in qualità di Titolare:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati (DPO);

e, relativamente a ciascun trattamento:

- le finalità del trattamento;
- struttura che ne è primariamente responsabile e Referente del Trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione relativa alla valutazione dell’adeguatezza delle garanzie;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Per i trattamenti svolti in qualità di Responsabile, il Registro contiene almeno le seguenti informazioni di carattere generale:

- il nome e i dati di contatto del Responsabile del trattamento e del responsabile della protezione dei dati (DPO);

e, relativamente a ciascun trattamento:

- il nome e i dati di contatto di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento;
- struttura che ne è primariamente responsabile e Referente del Trattamento;
- le categorie dei trattamenti effettuati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione relativa alla valutazione dell’adeguatezza delle garanzie;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

I trattamenti sono progettati ed implementati:

- in coerenza con i Principi di protezione dei dati personali (cfr infra);
- tenendo in considerazione la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i potenziali rischi per i diritti e le libertà delle persone fisiche interessate;
- operando in modo sinergico a quanto effettuato in conformità ad altre normative, a regolamenti specifici del settore bancario, in esito alle valutazioni di rischio.

5.2 Principi della protezione dei dati personali

La Banca è responsabile, nell'ambito dei trattamenti di propria competenza, del rispetto dei seguenti principi, garantendone la dimostrabilità:

a) liceità, correttezza e trasparenza - i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) limitazione della finalità - i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) minimizzazione dei dati - i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

d) esattezza - i dati devono essere 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

e) limitazione della conservazione - i dati devono essere 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, adottando misure tecniche e organizzative adeguate per tutelare i diritti e delle libertà dell'interessato

f) integrità e riservatezza - i dati devono essere 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

Base di liceità

I dati personali possono essere trattati solo dopo che il Titolare abbia identificato, stabilito ed attuato almeno una delle seguenti condizioni di liceità:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Valutazione di impatto (data protection impact assessment) e analisi dei rischi

Nei casi in cui i rischi sulla protezione dei dati personali relativi ad una o più attività di trattamento risultino particolarmente elevati (in base a criteri specificamente espressi dalla applicabile normativa o all'esito di valutazioni dei rischi), la Banca deve svolgere la valutazione di impatto (DPIA) e sottoporre la stessa al parere del Data Protection Officer, anche per valutare l'opportunità di sottoporre il trattamento a consultazione preventiva da parte della Autorità garante per la protezione dei dati personali.

L'opportunità dello svolgimento della Valutazione di impatto è presa in considerazione sia in fase di progettazione di un nuovo trattamento che, per quelli già in essere, ad ogni significativo cambiamento, sia tecnologico che organizzativo.

5.3 Adempimenti nei riguardi degli interessati del trattamento

Informative

L'interessato ha sempre diritto a ricevere una informativa adeguata, chiara, trasparente e completa nel descrivere i trattamenti che interessano i suoi dati personali, nel rispetto delle condizioni, tempistiche, modalità e contenuti stabiliti dalla applicabile normativa comunitaria e nazionale. E' responsabilità del Titolare e dei Responsabili del trattamento far si che l'Interessato riceva le Informative che riguardano i trattamenti svolti sui suoi dati personali.

Consenso

Nei casi in cui la base di liceità del trattamento preveda il consenso dell'interessato, il Titolare del trattamento direttamente o per tramite degli eventuali Responsabili deve:

- richiederlo in modo specifico e chiaramente distinguibile da altre eventuali dichiarazioni, richieste e condizioni presentate all'Interessato, in forma comprensibile e facilmente accessibile, consentendo a questi di esprimersi liberamente e senza condizionamenti nel conferire o meno il suo consenso
- consentire all'Interessato in qualunque momento di revocare un suo consenso precedentemente prestato, con la stessa facilità con la quale è stato accordato: ciò non pregiudica la validità dei trattamenti antecedenti alla revoca
- in caso di servizi on line specificamente offerti a minori, è necessario acquisire il consenso da parte del titolare della responsabilità genitoriale
- conservare prova di ogni consenso acquisito da un singolo Interessato
- definire e attuare misure e accorgimenti volti a garantire la non ambiguità del consenso.

Esercizio dei diritti degli Interessati

Il Titolare deve consentire agli Interessati l'esercizio dei loro diritti, ove applicabili al caso specifico di trattamento e rendere note le modalità con cui l'esercizio di tali diritti può essere richiesto.

Nel caso in cui si ritenga di non dovere (o non potere, ove possibile) rispondere positivamente alla richiesta, è comunque necessario fornire motivata risposta all'interessato.

I diritti in questione, come specificato dal Regolamento, riguardano:

- accesso
- rettifica, cancellazione (oblio) e relativo obbligo di notifica ad eventuali terzi ai quali i dati sono stati comunicati
- limitazione del trattamento
- portabilità
- opposizione
- opposizione a processo decisionale automatizzato profilazione inclusa.

5.4 Trattamenti particolari

Trattamento di dati particolari e giudiziari

Il trattamento di 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 o alla vita sessuale o all'orientamento sessuale della persona nonché di dati personali relativi a condanne penali e reati possono essere trattati solo ed esclusivamente:

1. per imprescindibili e documentate necessità legate al business e o all'amministrazione interna della singola società e
2. nel rispetto delle apposite prescrizioni a livello comunitario e nazionale in materia di protezione dati personali.

Controllo sulle finalità del trattamento

Qualora il Titolare di trattamento intenda utilizzare per altre finalità i dati personali precedentemente raccolti, è tenuto a verificare, preventivamente, che nel caso specifico ciò sia ammesso in base alle applicabili normative comunitarie e nazionali in materia di protezione dei dati personali, e sempre nel rispetto delle prescrizioni che riguardano la fornitura della Informativa ed esercizio dei diritti dell'Interessato.

Nei casi in cui, per motivi organizzativi, risulti necessaria nell'ambito di un trattamento la comunicazione di dati personali a soggetti terzi, questi ultimi sono selezionati in base a criteri di qualità e sono formalizzati gli impegni al mantenimento della protezione dei dati personali e le relative istruzioni in linea con la presente Politica, con i requisiti normativi applicabili e con gli accordi contrattuali.

5.5 Misure di sicurezza

La Banca in qualità di Titolare deve mettere in atto misure tecniche ed organizzative adeguate per attuare in modo efficace i principi ed integrare le garanzie volte a soddisfare i requisiti in materia di protezione dati personali portati dalla normativa comunitaria e quella nazionale, in considerazione dello stato dell'arte, costi di attuazione, natura, ambito di

applicazione, contesto e finalità di trattamento ed i relativi rischi per i diritti e le libertà delle persone fisiche.

Protezione dei dati personali fin dalla progettazione e per impostazione predefinita

Sin dalla fase di progettazione di un processo o servizio o applicazione che comporti trattamento di dati personali è necessario mettere in atto misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a personale non dotato di specifiche autorizzazioni.

Formazione

La Funzione DPO, in collaborazione con la Segreteria Generale, identifica su base annuale il fabbisogno di attività formative in materia di protezione dei dati personali da erogare al personale interessato (Referenti del Trattamento, Incaricati, Amministratori di Sistema) e propone le relative attività nell'ambito del Piano di Formazione.

La Direzione Generale, nella figura del Direttore Generale, con il supporto della Segreteria Generale, provvede alla pianificazione ed erogazione delle connesse attività di formazione.

Gestione delle violazioni di sicurezza dei dati personali

La gestione delle violazioni di sicurezza rientra nell'ambito più generale della gestione degli incidenti.

La Banca opera al fine di prevenire violazioni di sicurezza nelle quali siano coinvolti dati personali e deve attuare opportuni presidi tecnologici ed organizzativi al fine di rilevare quanto prima eventi che possano rappresentare incidenti di sicurezza.

Nei casi in cui l'analisi di un incidente di sicurezza porti ad avere certezza o probabilità di una violazione di dati personali che possa rappresentare rischi per i diritti e le libertà delle persone fisiche interessate, anche con particolare riguardo ai dati sensibili, e giudiziari e biometrici, la classificazione dell'incidente deve essere adeguata all'attivazione delle procedure di escalation previste per i "Gravi incidenti di sicurezza informatica".

Deve essere tempestivamente interessato il DPO che, in collaborazione con il Referente Interno Data Protection Officer, provvede a valutare la fondatezza della violazione e l'opportunità di avviare procedure di segnalazione all'Autorità Garante ed agli interessati.

Tale comunicazione al Garante ed all'interessato (quando la violazione dei dati personali risulti suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche) deve essere effettuata tempestivamente, e comunque non oltre entro 72 ore dalla conoscenza del fatto.

Trasferimenti di dati verso paesi terzi (extra UE) o organizzazioni internazionali

La comunicazione di dati personali a soggetti terzi al di fuori dell'Unione Europea, per i quali la Commissione Europea non abbia emesso un giudizio di adeguatezza delle tutele per i dati personali, è preventivamente vagliata, anche al fine di verificarne la liceità e l'opportunità di ottenere specifiche autorizzazioni, e sono adottate adeguate misure atte a garantire la protezione dei dati, tra cui formali ed adeguati accordi contrattuali.

5.6 Miglioramento continuo

È impegno dei vertici aziendali il raggiungimento ed il mantenimento degli obiettivi in materia di protezione dei dati personali, in un'ottica di continuo miglioramento.

L'adeguatezza nel continuo della presente Politica è verificata con frequenza almeno annuale.

6. MODELLO ORGANIZZATIVO

Al fine di assicurare l'implementazione ed il governo di quanto necessario per la corretta gestione dei trattamenti di dati personali, il Modello organizzativo della Banca prevede:

- l'articolazione delle responsabilità indicate dal dettato normativo come di competenza del Titolare/Responsabile di trattamento;
- l'attribuzione di specifiche responsabilità e compiti connessi ai trattamenti di dati personali agli addetti incaricati di tali trattamenti;
- le modalità di designazione e controllo dei "Responsabili del trattamento dei dati", (ossia i soggetti esterni, come ad esempio gli outsourcers) a cui attribuire specifici compiti e fornire istruzioni mediante contratti;
- l'assegnazione del ruolo e delle connesse responsabilità dei Referenti del Trattamento, ovvero i soggetti che assicurano il rispetto della normativa, in relazione a ciascun trattamento. Sono nominati Referenti del Trattamento tutti i responsabili di processo nell'ambito del quale il trattamento viene effettuato;
- le modalità di designazione e controllo degli "Amministratori di Sistema".
- l'assegnazione ad Iccrea Banca della Funzione DPO per l'assolvimento dei compiti ad essa assegnati per dettato normativo, nell'ambito dell'adesione al Servizio erogato da Iccrea Banca;
- l'assegnazione del ruolo di Referente Interno DPO, individuato nel Referente interno Compliance, con il compito di supportare per quanto di propria competenza le attività del DPO;
- la nomina di Iccrea Banca quale Responsabile dei trattamenti connessi all'attività di DPO.

7. RUOLI PRINCIPALI

Nel seguito, vengono illustrate le responsabilità attribuite alle figure previste dalla normativa o la cui definizione sia ritenuta opportuna per l'ottimale articolazione di responsabilità.

Titolare del trattamento

Il "Titolare del trattamento" è la persona giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali e che ha la responsabilità di:

- mettere in atto misure tecniche e organizzative adeguate (e riesaminate ed aggiornate qualora necessario) per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al Regolamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle

persone fisiche; tra esse vi è l'attuazione di politiche adeguate in materia di protezione dei dati;

- designare il Data Protection Officer;
- valutare l'adesione a codici di condotta o a meccanismi di certificazione come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Tale ruolo è ricoperto dal Consiglio di Amministrazione che:

- delibera e approva la politica e la normativa interna in tema di "Protezione dei Dati Personali" di attuazione della normativa vigente nonché l'assegnazione dei compiti alle diverse strutture in essa prevista;
- designa il Data Protection Officer, ne definisce i compiti e ne assicura indipendenza e disponibilità di risorse;
- approva il Piano delle verifiche sul rispetto delle prescrizioni della normativa esterna ed interna nell'ambito dei trattamenti svolti internamente o esternamente tramite Responsabili di trattamento;
- acquisisce le risultanze delle verifiche periodiche e dispone gli interventi necessari alla sistemazione delle anomalie riscontrate;
- esercita, direttamente o indirettamente, le competenze di cui al prossimo capoverso.

Al fine di assicurare un adeguato livello di efficacia al processo di protezione dei dati personali, il Titolare può conferire mediante delibera autorizzata dal Consiglio di Amministrazione alcune specifiche deleghe quali ad esempio:

- approvare la nomina di soggetti esterni quali Responsabili di Trattamento;
- incaricare soggetti interni ed esterni quali autorizzati al trattamento;
- designare soggetti interni ed esterni quali Amministratori di Sistema;
- fornire le direttive in tema di sicurezza fisica ed informatica per garantire la protezione dei dati personali;
- fornire le istruzioni a cui i Responsabili di Trattamento, i Referenti del Trattamento, gli Incaricati del trattamento e gli Amministratori di Sistema devono attenersi nell'ambito della nomina ricevuta;
- autorizzare nuovi trattamenti resisi necessari per l'operativa della società;
- sottoscrivere le risposte alle richieste ordinarie provenienti dal Garante o da altre Autorità di Controllo;
- esercitare ogni azione a tutela dei dati della società;
- approvare ulteriori regolamenti interni e procedure operative necessari alla gestione delle attività in materia di protezione dei dati personali.

DATA PROTECTION OFFICER

Il ruolo di Data Protection Officer è esternalizzato a Iccrea Banca sulla base del contratto di servizio stipulato con la stessa. La Banca identifica il Referente Data Protection Officer.

Oltre ai compiti di seguito indicati, il DPO ha la responsabilità di monitorare la corretta implementazione e conservazione del "Registro delle attività di trattamento".

Compiti del Data Protection Officer:

- informa e fornisce consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorveglia l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;
- coopera con l'autorità di controllo;
- supporta la gestione del "Registro delle attività di Trattamento";
- partecipa alle valutazioni relative a violazioni di sicurezza di dati personali;
- gestisce, ove opportuno in collaborazione con il Referenti DPO ed i Referenti dei trattamenti interessati, le richieste di accesso ai dati personali e di esercizio dei propri diritti da parte degli interessati.

Responsabile del Trattamento

Qualora la Banca affidi a soggetti esterni trattamenti di dati personali, questi sono designati Responsabili del trattamento (ad esempio outsourcers presso i quali sono esternalizzati trattamenti di dati personali).

La Banca, in qualità di Titolare, fornisce ai Responsabili del trattamento istruzioni affinché gli stessi promuovano l'adozione di prassi conformi al Regolamento e alle correlate norme interne di attuazione, organizzando e conducendo le attività di competenza in modo da garantire adeguati requisiti di correttezza e sicurezza dei trattamenti effettuati.

Incaricato al trattamento

L'Incaricato al trattamento è la persona fisica che, nell'ambito della normativa sulla protezione dei dati personali, in funzione di un'apposita designazione scritta e sotto la diretta autorità del Titolare e, eventualmente, del Referente del Trattamento, effettua materialmente le operazioni di trattamento sui dati personali.

In base a questa nomina, ferma restando la mansione aziendale assegnata, al fine di assicurare le misure minime di sicurezza previste dal Codice per i trattamenti di propria competenza, l'Incaricato è tenuto ad osservare le istruzioni contenute nella lettera di incarico e nei relativi allegati nonché i seguenti compiti ad integrazione di quanto già previsto da specifiche normative interne.

In particolare, l'Incaricato deve:

- trattare i dati personali unicamente nell'ambito delle finalità e delle modalità del trattamento attribuite dalla Banca all'unità organizzativa di appartenenza e limitatamente allo svolgimento delle proprie mansioni operative;
- far circolare i dati personali esclusivamente tra i dipendenti che ne abbiano necessità per esigenze di lavoro nell'ambito della UO di appartenenza ovvero delle altre UO previste dalle norme e dalle procedure stabilite dalla Banca;

- segnalare al proprio Responsabile o Referente del Trattamento eventuali trattamenti non esplicitamente previsti dalla lettera di incarico che l'esperienza faccia però ritenere indispensabili per lo svolgimento delle responsabilità operative;
- garantire la riservatezza dei dati personali trattati per lo svolgimento della propria attività lavorativa, facendosi parte attiva nella segnalazione di eventuali situazioni anomale;
- trattare i dati personali acquisiti nel rispetto delle norme e delle procedure stabilite dalla Banca nell'ambito delle quali è prevista la corretta resa dell'informativa al soggetto interessato e la raccolta del suo consenso al trattamento, se necessario;
- accedere ai dati personali, tramite risorse informatiche come previsto nelle normative di processo applicabili.

Per ogni dubbio che dovesse sorgere in merito a quanto appena rappresentato, gli incaricati sono tenuti a rivolgersi ai Referenti del Trattamento di competenza.

Incaricato esterno al trattamento

Le attività di trattamento dei dati svolte internamente dalla Banca possono essere assegnate, oltre che al personale dipendente ("Incaricato al trattamento"), anche a personale di Aziende Esterne ("Incaricato esterno al trattamento")[1].

Condizione necessaria per l'attribuzione di tali abilitazioni è la nomina della Società Esterna quale Responsabile di trattamento.

I compiti dell'Incaricato Esterno al trattamento possono essere anche ulteriormente limitati o specificati per uno o più incaricati, assicurandone la coerenza con l'oggetto della prestazione prevista nell'accordo contrattuale con l'azienda fornitrice del servizio.

In base a quanto contenuto nell'atto di designazione, l'Incaricato esterno è tenuto ad osservare le istruzioni che il Responsabile ha impartito sulla base del contenuto del servizio reso nei confronti del Titolare del trattamento previsto nell'accordo contrattuale.

Amministratore di Sistema

Con il provvedimento del 27/11/2008[2], il Garante ha individuato le figure degli Amministratori di Sistema come "figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di suoi componenti, "gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi" indicando anche le relative aree di attività.

Le varie figure professionali complessivamente indicate come "Amministratore di Sistema" ai fini del provvedimento in esame, nella realtà operativa della Banca possono essere quindi così individuate:

- nell'ambito delle attività di gestione operativa:
    - amministratori di impianti di elaborazione (sistemi operativi e loro componenti, inclusi prodotti software di base);
    - amministratori di basi di dati;
    - amministratori di reti e di apparati di sicurezza;
    - amministratori di dati;

[1] Non sono qui ricompresi gli addetti che svolgono attività di trattamento presso i Responsabili Esterni.
[2] "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

  - amministratori di sistemi software complessi (quali applicazioni costituite da componenti separate per interfaccia utente, logica elaborativa, accesso ai dati);
- nell'ambito delle attività di gestione delle applicazioni:
  - assegnatari di temporanei privilegi di accesso straordinari, dovuti alla necessità di intervento per ripristinare la disponibilità e/o l'integrità di dati o all'assistenza durante le fasi di aggiornamento del software;
  - assegnatari delle utenze di amministrazione delle applicazioni e/o delle cosiddette utenze applicative, in base alla considerazione che tali utenze permettono "specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati" e che tali criticità sono di norma accresciute dalle capacità di "comprensione del dominio applicativo" detenute dagli assegnatari;
- attività analoghe a quanto sopra descritto svolte da dipendenti nell'ambito di trattamenti il cui Titolare sia una diversa Società che abbia nominato la Banca "Responsabile".

Sono individuati, tra i trattamenti di amministrazione di "informazioni di carattere personale dei lavoratori", le attività di gestione delle applicazioni e dei sottostanti sistemi informatici di utilizzo delle Unità Organizzative adibite alle seguenti aree (in relazione alla possibilità di detto personale di trovarsi a trattare "anche dati personali riferiti ai lavoratori operanti nell'ambito dell'organizzazione" o di essere "nella condizione di acquisire conoscenza di dati ad essi riferiti"[3]):

- gestione e amministrazione del personale;
- gestione della contabilità e bilancio per la parte relativa a paghe e contribuzioni;
- gestione del servizio di posta elettronica e di navigazione Internet;
- gestione delle risorse informatiche assegnate (ad es. PC, telefoni);
- gestione dei sistemi di videosorveglianza e/o videoregistrazione;
- gestione di conti correnti e/o portafogli finanziari e/o crediti e finanziamenti che possano comprendere posizioni intestate a personale dipendente
- gestione di movimenti contabili (ad es. SCT/SDD, movimenti su carte di pagamento) che possano interessare i conti correnti intestati a personale dipendente.

Per le predette figure, il Garante prescrive a carico del Titolare i seguenti adempimenti obbligatori:

- valutazione delle caratteristiche soggettive;
- designazione individuale;
- Mantenimento[4] dell'elenco degli Amministratori di Sistema;
- registrazione degli accessi;
- verifica delle attività svolte.

Le funzioni di Amministratore di Sistema possono essere assegnate, oltre che al personale dipendente ("Amministratore di Sistema Interno"), anche a personale di Aziende Esterne che necessitasse, per lo svolgimento di attività contrattualizzate, di eseguire trattamenti

[3] cfr. FAQ 2 al citato provvedimento

[4] Nel caso di trattamenti in "outsourcing", tale compito può anche essere svolto dal Responsabile esterno (cfr. aggiornamento contenuto nel Provvedimento del 25 giugno 2009)

quali quelli sopra descritti ("Amministratore di Sistema Esterno"). Condizione necessaria per l'attribuzione di tali abilitazioni è la nomina della Società Esterna quale "Responsabile" di trattamento.

L'Amministratore di Sistema è tenuto al rispetto dei compiti precedentemente descritti, a seconda della propria qualifica di Incaricato al trattamento.

Con riferimento alle responsabilità ed ai compiti delle principali funzioni aziendali nell'ambito del comparto Privacy si rimanda ai contenuti del Regolamento di processo.