Policy di Data Governance

Consiglio di Amministrazione di Flowe del 28/03/2023

Indice generale

1 Premessa

Scopo del presente documento è fornire una descrizione dei principi adottati da Flowe S.p.A. Società Benefit (di seguito anche Flowe o la Società) in tema di Data Governance.

1.1 CONTESTO DI RIFERIMENTO

Il sistema di gestione dei dati riveste un ruolo fondamentale per consentire all'azienda di prendere le decisioni strategiche e manageriali sulla base di informazioni aggiornate, complete, attendibili e fruibili. La "Data Governance" è l'insieme di processi, ruoli, Policy, standard e metriche definiti al fine di favorire un uso efficace ed efficiente delle informazioni, al fine di raggiungere gli obiettivi prefissati, attraverso l'implementazione di un framework di gestione dei dati applicabile progressivamente a tutti gli ambiti informativi aziendali.

1.2 AMBITO DEL DOCUMENTO

La presente Policy descrive i principi adottati da Flowe ed ispirati a quelli della capogruppo Banca Mediolanum, per il presidio dei modelli, dei processi e delle procedure finalizzati al governo, nel continuo, del patrimonio informativo aziendale.
I principi richiamati nella presente Policy trovano quindi attuazione nelle linee guida operative e nei regolamenti di processo, nei quali saranno meglio declinati i compiti, le attività operative e di controllo, alla base del rispetto degli adempimenti relativi alle normative.

Tali regolamenti descriveranno più nel dettaglio gli ambiti di applicazione in termini di Data Architecture, Data Quality e Data Protection, gli attori coinvolti, i loro ruoli e le responsabilità all'interno della Società.

1.3 GERARCHIA DELLE FONTI

Con riferimento alla "Policy di Conglomerato sulle modalità di redazione, aggiornamento, approvazione e diffusione della Normativa Interna", il presente documento si colloca al primo livello (di vertice) della piramide documentale richiamata nello schema seguente:

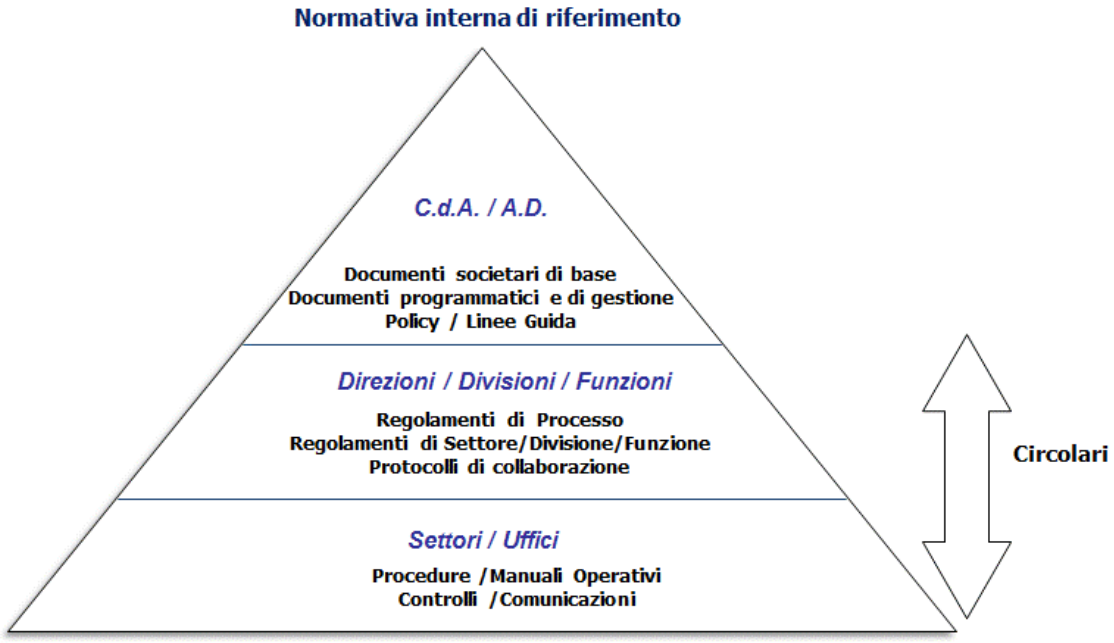

Figura 1. Modello della Normativa Aziendale

2 Applicabilità

2.1 DESTINATARI DEL DOCUMENTO

Il presente documento è approvato dal Consiglio di Amministrazione di Flowe e trova diretta applicazione all'interno della Società. La presente Policy è ispirata ai principi della omologa Policy della capogruppo Banca Mediolanum, recepiti tenendo conto delle specificità e in base a criteri di proporzionalità, in sintonia con le specifiche disposizioni di settore emanate dalle Autorità di Vigilanza[1] e la propria regolamentazione interna.

2.2 RESPONSABILITÀ DEL DOCUMENTO

L'aggiornamento e la revisione del presente documento sono di responsabilità della Perspective Organization & Business Continuity.

Ogni modifica o integrazione sostanziale del Documento deve essere approvata dal Consiglio di Amministrazione della Società.

3 Definizioni

Termine	Definizione
Ambito Informativo	Insieme di Categorie Informative omogenee

[1] Provvedimento Banca d'Italia n. 74/22 del 22/2/2022 che modifica le «Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica» del 17 maggio 2016 come modificato dal provvedimento del 23 luglio 2019.

Termine	Definizione
Architettura	Concetti fondamentali o proprietà di un sistema nel suo ambiente incentrati nei suoi elementi, relazioni e nei principi del suo disegno ed evoluzione)
Categoria Informativa	Insieme di più Oggetti Informativi
Dataset	Definisce un insieme strutturato di dati coerente rispetto ad uno specifico ambito informativo
Dato	Rappresentazione reinterpretabile dell'informazione in un modo formalizzato idoneo per la comunicazione, l'interpretazione o l'elaborazione
Dizionario dei Metadati	Mappatura tecnica del patrimonio informativo rilevante per il governo di dati
Glossario di Business	Descrizione a livello di semantica funzionale del patrimonio informativo della Società
Informazione	Conoscenze riguardanti oggetti, come fatti, eventi, cose, processi, o idee, compresi concetti, che all'interno di un determinato contesto hanno un significato particolare
Key Quality Indicator (KQI)	Misura della qualità del dato che consente di rendere efficaci, analizzabili ed interpretabili i controlli effettuati in funzione dell'obiettivo definito
Mappa dei Dati	Insieme delle caratteristiche che descrivono i flussi dati e i dati che li compongono, coerentemente con il ciclo di vita del dato e con i processi di estrazione, trasformazione e caricamento del dato (processo elaborativo del dato)
Metadato	Dato che descrive altri dati
Oggetto Informativo (OI)	Report, aggregazioni, flussi informativi, applicazioni, basi dati interne ed esterne ecc…) che identificano l'unità informative elementari utilizzate per rappresentare il patrimonio informativo aziendale da un punto di vista di business
Procedura Informatica	Insieme di applicativi funzionali alla ricezione di dati, al controllo di flussi di dati (Diagnostico), all'archiviazione temporanea o permanente di dati (Base dati o archivio Elettronico), all'elaborazione di dati (Motore di calcolo), all'estrazione di flussi di dati / report (Estrattore)
Reporting	Flussi di dati elettronici o manuali prodotti, di norma, per essere utilizzati dalla struttura organizzativa destinataria senza la necessità di ulteriori elaborazioni. Report complessi, per essere letti, possono necessitare di procedure informatiche appositamente dedicate

Termine	Definizione
Sistema	Insieme di differenti procedure informatiche interconnesse da scambi di flussi di dati. Un sistema può essere articolato in più sotto-sistemi. Una procedura informatica può appartenere a più sistemi (o sotto-sistemi) in funzione di flussi di dati scambiati con altre procedure informatiche. Si parla, inoltre, di Sistema Alimentante per identificare il sistema dove ha origine il dato che viene scambiato con il Sistema Ricevente che ne richiede l'estrazione e l'utilizzo
Sistema di sintesi	Sistema informatico alimentato da flussi di dati provenienti da diverse procedure sezionali al fine di elaborare informazioni aggregate di sintesi, strutturate in report direzionali o gestionali o ulteriori flussi di dati
Sistema Informatico	Sistema contenente una o più componenti hardware, software e dati associati
Sistema Informativo	Uno o più sistemi informatici e sistemi di comunicazione, assieme alle risorse organizzative associate come risorse umane, tecniche e finanziarie che forniscono e distribuiscono le informazioni

4 Ruoli e responsabilità

Il Modello di Data Governance adottato per la gestione e il presidio della qualità dei dati prevede il coinvolgimento degli organi e delle unità organizzative descritte di seguito, nonché delle unità organizzative e delle risorse della Società a vario titolo coinvolte nei processi di alimentazione, elaborazione e produzione dei dati rilevanti di cui si compone il patrimonio informativo aziendale, alle quali sono attribuiti i ruoli e le responsabilità definite nel successivo paragrafo 5.2.

Ogni dipendente, nel rispetto alle proprie mansioni e attività, è responsabile della corretta imputazione, utilizzo e trattamento dei dati disponibili attraverso sistemi di informatica individuale o sistemi informatici centralizzati.

Specifiche responsabilità sono assegnate per le fonti di dati rilevanti che entrano a far parte del perimetro a livello appropriato e collocando puntualmente le attività secondo il modello organizzativo adottato.

4.1 CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione è responsabile dell'adozione della presente Policy e della delibera dei successivi aggiornamenti.

4.2 AMMINISTRATORE DELEGATO

L'Amministratore Delegato viene aggiornato con cadenza annuale, tramite apposita relazione, sulla situazione complessiva del modello di Data Governance e di qualità dei dati, da parte della Perspective Organization & Business Continuity.

4.3 COMITATO DI INFORMATION GOVERNANCE DI BANCA MEDIOLANUM

Il Comitato Information Governance della Capogruppo ha funzione consultiva e propositiva di ausilio al buon funzionamento delle attività di governo dei dati della Banca e delle società controllate, a garanzia della complessiva qualità delle informazioni. Tale Comitato si riunisce di norma con periodicità trimestrale, salvo casi di diversa necessità.
Il comitato, in particolare:

- propone l'indirizzo delle strategie aziendali in materia di Information Governance, presidiando la declinazione del framework di Data Governance e di Data Analytics sull' intera organizzazione;
- definisce il perimetro di applicazione del framework di Data Governance e di Data Analytics, necessità e i piani per la sua estensione nel tempo;
- assicurare un livello di comprensione delle tematiche di Data Governance condiviso tra le strutture;
- definisce il quadro di riferimento per l'aggregazione e la reportistica dei dati di rischio a livello di Gruppo Bancario secondo i principi BCBS239;
- assicura un livello di comprensione delle tematiche di Information Governance condiviso tra le strutture organizzative
- valuta la corretta attribuzione dei ruoli e responsabilità nell'ambito del framework di Information Governance definito, con particolare riferimento ai Data Owner anche in ottica di prevenzione dei rischi, per i dati ricompresi nel perimetro di applicazione;
- definisce i piani di intervento in materia di Data Governance, con particolare riferimento ai dati di rischio;
- valuta gli impatti della normativa di settore sul modello di Data Governance e Data Analitycs adottato;
- aggiorna i criteri di rilevanza dei dati ed esprime valutazioni sulla corretta attribuzione del grado di rilevanza dei dati ricompresi nel perimetro di applicazione;
- garantisce che le funzioni aziendali di controllo siano informate sul sistema di gestione dei dati;
- esamina preventivamente la relazione annuale verso l'Amministratore Delegato, il Comitato Rischi e il Consiglio di Amministrazione sulla situazione complessiva della Data

Governance aziendale e in particolare sull'efficace aggregazione e reportistica dei dati di rischio;

- valuta l'adeguatezza del sistema di controllo dei dati;
- supervisiona gli esiti dei Remediation Plan;
- esprime alle società controllate eventuali "Binding opinion"/ "Non binding opinion".

Il Comitato Information Governance è composto da:

- Chief Data & Analytics Officer (ruolo svolto dal Responsabile Pianificazione e Controllo), che assume anche il ruolo di Presidente;
- Responsabile Unità di Data Governance;
- Direttore Generale;
- Chief Financial Officer;
- Responsabile Risk Management;
- Responsabile Service, Operations & ICT;
- Responsabile Credito;
- Responsabile Portafoglio Progetti & Sviluppo Organizzativo;
- Responsabile Organizzazione e Project Management;
- Responsabile ICT (CIO);
- Responsabile IT & Security Governance (CISO);
- Data Value Management.

Alle riunioni del Comitato Information Governance possono partecipare, oltre ai suoi membri, a titolo consultivo e di supporto:

- Responsabile Compliance;
- Responsabile Audit;
- Responsabili delle Direzioni / Divisioni / Unità Organizzative rilevanti, in funzione degli argomenti;
- Esponenti aziendali di Società del Gruppo, inteso anche come Conglomerato Finanziario, in funzione degli argomenti.

4.4 UNITÀ ORGANIZATION & BUSINESS CONTINUITY

La Perspective Organization & Business Continuity è responsabile del disegno, implementazione e manutenzione del Sistema di governo dei dati della Società, al fine di favorire il passaggio da un approccio di gestione del dato, dettato dalle necessità di controllo e conformità alla normativa, ad un approccio di valorizzazione del patrimonio informativo bancario, abilitando il Gruppo all'utilizzo strategico del dato stesso.

La Perspective Organization & Business Continuity definisce e manutiene il Sistema di Gestione dei dati interno, attraverso l'identificazione di ruoli, responsabilità, processi e strumenti atti a garantire

la gestione efficace ed efficiente del patrimonio informativo del Gruppo e le relative attività di reporting verso gli organi competenti. Di seguito le principali responsabilità:

- supportare il Comitato di Information Governance di Banca Mediolanum nella gestione, coordinamento e indirizzamento delle tematiche di Data Governance, in linea con la normativa vigente e gli indirizzi strategici del Gruppo, nella declinazione e verifica dell'attuazione del modello di Data Governance, nonché nella raccolta e condivisione delle informazioni necessarie al processo decisionale per l'attribuzione dei ruoli e responsabilità, nella valutazione della rilevanza dei dati per la definizione ed il monitoraggio delle azioni necessarie a garantire il governo delle informazioni, in particolare negli ambiti a maggiore rischio. Partecipa, inoltre, alle riunioni operative del Comitato;
- definire e aggiornare la normativa interna sulla base della Strategia di Data Governance;
- valutare, seguendo gli indirizzi definiti dal Comitato, l'adeguatezza ed efficacia dei presidi e delle misure di qualità dei dati, fornendo supporto metodologico ai Data Owner nella identificazione degli obiettivi e dei controlli in funzione del rischio di mancata qualità dei dati;
- recepire le indicazioni della Capogruppo su tematiche relative alla valorizzazione strategica del dato;
- collaborare con i data owner nelle attività di censimento, valutazione della rilevanza dei dati aziendali ed indirizzamento dei presidi e dei controlli per la copertura dei rischi identificati;
- fornire indirizzi all'Unità Data della Perspective Augmented Intelligence nell'individuazione ed implementazione delle soluzioni volte a garantire la qualità dei dati, mediante la formalizzazione dei requisiti di progettazione ed evoluzione dell'architettura di gestione dei dati e della relativa roadmap implementativa;
- identificare, valutare e promuovere all'interno dell'azienda gli strumenti atti a supportare il tracciamento dei controlli di qualità, il monitoraggio dei relativi risultati anche tramite la definizione dei Key Quality Indicator, e il reporting dei relativi esiti agli utenti di business, alle funzioni di controllo ed al management dell'azienda;
- supportare la Funzione Compliance nella valutazione periodica e nel conseguimento della conformità alle normative con impatti diretti sulla Data Governance e sulla qualità dei dati, analizzando gli impatti, nonché identificando e coordinando gli interventi di adeguamento;
- monitorare il portafoglio delle iniziative aziendali, valutandole e caratterizzandole sulla base del rischio di perdita di qualità del dato, al fine di indirizzare l'attuazione di

adeguati presidi e supportare le funzioni aziendali coinvolte nell'identificazione dei requisiti di gestione e controllo dei dati e nelle diverse fasi realizzative;

- relazionare all'Amministratore Delegato ed al Comitato di Information Governance di Banca Mediolanum sulla qualità dei dati e sullo stato di adozione del modello di Data Governance, sulla base delle informazioni raccolte dalle diverse funzioni aziendali coinvolte, producendo la relazione annuale all'Amministratore Delegato sulla situazione complessiva dello stato di adozione del modello di Data Governance e della qualità dei dati;
- effettuare la verifica, con cadenza almeno annuale, della conformità dell'operatività aziendale con la politica di Data Governance, orientata all'individuazione degli opportuni interventi e iniziative di miglioramento dell'efficacia ed adeguatezza del sistema;
- definire la procedura operativa per le attività in ambito, in linea con gli indirizzi e il perimetro di dati definito dal Comitato di Information Governance;
- presidiare la conformità delle evoluzioni di architettura dati rispetto agli standard e ai principi di Data Governance avvalendosi del supporto delle altre perspective se necessario;
- coordinare le attività ed i processi all'interno della Società inerenti all'implementazione del framework di data governance, costituendo il raccordo tecnico fra i System Owner responsabili dei singoli ambiti applicativi.

4.5 FUNZIONE RISK MANAGEMENT

La Funzione Risk Management, nell'ambito delle attività di governo dei dati, ha la responsabilità di indirizzare le politiche di gestione e controllo dei rischi inerenti alla qualità dei dati della Banca. A tal fine, partecipa, a titolo consultivo e di supporto, al Comitato di Information Governance di Banca Mediolanum.

4.6 FUNZIONE COMPLIANCE

La Funzione Compliance, nell'ambito delle attività di governo dei dati, ha la responsabilità di eseguire le verifiche di adeguatezza dei presidi organizzativi (processi, strutture e controlli) in ambito Data Governance, in accordo con il sistema di controllo interno adottato (controlli di 2° livello). Partecipa, a titolo consultivo e di supporto, al Comitato di Information Governance di Banca Mediolanum.

4.7 FUNZIONE INTERNAL AUDIT

La Funzione Internal Audit, nell'ambito delle attività di governo dei dati, ha la responsabilità di eseguire, relativamente al sistema di controllo interno adottato, le verifiche ed i controlli di 3° livello sul modello e sui processi di Data Governance. Partecipa, a titolo consultivo e di supporto, al Comitato di Information Governance di Banca Mediolanum.

4.8 PERSPECTIVE AUGMENTED INTELLIGENCE

La Perspective Augmented Intelligence implementa l'applicazione del framework complessivo di Data Governance per il perimetro applicativo individuato, attraverso le proprie strutture competenti.

4.8.1 Data

L'Unità Data, all'interno della Perspective Augmented Intelligence, ha responsabilità di definire gli strumenti in materia di Data Governance.

Inoltre, ha la responsabilità di:

- supportare l'Unità Organization & Business Continuity e i data owner nell'identificare gli interventi per il miglioramento del livello di qualità del dato;
- individuare le soluzioni tecniche volte a garantire la qualità tecnica dei dati sulla base degli indirizzi forniti dalla Perspective Organization & Business Continuity .

4.8.2 IT Operation Security & Governance

L'Unità IT Operation Security & Governance all'interno della Perspective Augmented Intelligence indirizza le misure di protezione dei dati in funzione del livello di classificazione, in carico ai Data Owner degli stessi in termini di disponibilità, riservatezza ed integrità.

5 Principi in materia di Data Governance

L'evoluzione del quadro normativo in atto è caratterizzata dalla crescente rilevanza attribuita ai dati e al loro contenuto informativo quali elementi fondamentali a supporto delle decisioni strategiche e operative e, in definitiva, del corretto funzionamento delle aziende. Tale impostazione a livello regolamentare risente anche delle principali tendenze di mercato caratterizzate, negli ultimi anni, da una forte spinta innovativa.

In tale contesto, il patrimonio informativo rappresenta per le aziende un'importante risorsa, la cui gestione non ottimale potrebbe comportare l'esposizione a rischi (operativi, di conformità e reputazionali).
Il Modello di Data Governance ha quindi l'obiettivo di assicurare che la Società disponga di dati affidabili e pienamente adeguati allo scopo per cui saranno utilizzati.

In tale contesto, il Modello:

- definisce gli ambiti e le strategie di applicazione dei principi di Data Governance;
- individua i ruoli e le responsabilità nel trattamento delle informazioni aziendali;
- definisce i processi, i metodi e gli strumenti attuativi dei principi di Data Governance;
- supporta i processi aziendali nel presidio delle caratteristiche inerenti alla qualità del dato, per limitare eventuali impatti in termini di rischio (operativo, di compliance, reputazionale), indirizzando l'implementazione dei presidi di Data Governance all'interno dei progetti aziendali con impatti sui dati (Data Governance "by design");
- garantisce l'applicazione continuativa nel tempo della Data Governance;
- promuove all'interno della Società la consapevolezza della centralità del dato e dei principi di Data Governance nei processi aziendali.

5.1 AMBITI DI DATA GOVERNANCE

Il Modello di Data Governance prevede l'identificazione di ruoli, responsabilità, processi e strumenti atti a garantire la gestione efficace ed efficiente del patrimonio informativo della Società e le relative attività di reporting verso gli organi competenti.
Sulla base di tali principi, la Perspective Organization & Business Continuity sviluppa le linee guida del Governo dei Dati della Società lungo le seguenti direttrici:

- Data Quality Management che consiste nell'insieme delle azioni/misure finalizzate a verificare il livello di qualità dei dati rispetto a requisiti predefiniti (normativi e/o gestionali) e rispetto a specifiche dimensioni di qualità del dato;
- Data Management (declinato in termini di Data Protection e Data Architecture) che consiste nell'insieme delle azioni/misure volte alla gestione e alla manutenzione del dato sin dalla sua creazione/acquisizione, fino alla sua trasformazione, utilizzo, archiviazione.

Al fine di gestire in modo efficace le attività in ambito Data Governance, Flowe ha deciso di adottare un framework a livello di Gruppo coordinato dalla Capogruppo e declinato secondo i seguenti ambiti:

- **Data Quality**;
- **Data Protection**;
- **Data Architecture**.

5.1.1 Data Quality

La Data Quality disciplina il modello di gestione della qualità dei dati, al fine di garantire che la registrazione degli eventi aziendali e le informazioni utilizzate per la strutturazione di rapporti e informative verso i mercati e gli organi di vigilanza sia eseguita in modo da soddisfare i seguenti principi: accuratezza, coerenza, completezza, conformità formale, compliance, riservatezza, integrità, tempestività, univocità, trasparenza, pertinenza, accountability, verificabilità, coerenza tecnica.

In particolare, la Data Quality definisce:

- gli obiettivi e i criteri di valutazione della qualità dei dati;
- il processo di qualità dei dati;
- i controlli, le metriche e gli indicatori per la misurazione della qualità dei dati;
- il processo di monitoraggio e reporting dei risultati di analisi della qualità dei dati.

I controlli sulle registrazioni contabili devono verificare, tra l'altro, le procedure per l'individuazione e sistemazione delle divergenze tra saldi dei sottosistemi sezionali e quelli della contabilità generale, i processi di quadratura tra i documenti di front-office e le registrazioni giornaliere; la conferma periodica dei rapporti con controparti e clienti. Le verifiche devono riguardare anche l'allineamento tra i dati utilizzati per la gestione dei rischi e per la rendicontazione finanziaria.

Per i dati che contribuiscono alla definizione del profilo di rischio della Società, il sistema di gestione dei dati assicura che le informazioni siano complete e aggiornate. Le strutture aziendali coinvolte nella definizione del profilo di rischio della Società devono esplicitare le principali assunzioni e gli eventuali criteri di stima adottati nella produzione dei report che hanno rilevanza ai fini regolamentari.

5.1.2 Data Protection

La Data Protection è orientata all'individuazione dei requisiti e all'indirizzamento delle misure di protezione dei dati, con l'obiettivo di garantire gli adeguati livelli di riservatezza, integrità e disponibilità in funzione della finalità d'uso. Nel dettaglio, la Data Protection indirizza i seguenti principi:

- **Riservatezza**: l'accesso ai dati deve essere consentita solo ai soggetti autorizzati, secondo il principio di *need to know*, limitando al contempo un utilizzo dei dati improprio o effettuato da soggetti non autorizzati.
- **Integrità:** deve essere garantita la protezione dei dati rispetto a cancellazioni o modifiche di informazioni non autorizzate, sia a seguito di fatti accidentali o naturali, sia di atti dolosi.
- **Disponibilità:** deve essere garantita l'accessibilità dei dati nel rispetto delle necessità di utilizzo da parte dei soggetti autorizzati.

Il Modello di Data Governance ha l'obiettivo di definire i criteri e le modalità di classificazione della criticità dei dati sulla base di caratteristiche di tipo normativo, di business e di sicurezza e dei relativi rischi (es. operativo, di compliance, reputazionale) legati alla perdita di riservatezza, integrità e disponibilità.

I Processi, i metodi e gli strumenti definiti a livello aziendale per garantire il soddisfacimento dei principi di Data Protection sono declinati in apposite linee guida e / o procedure operative di realizzazione del Modello di Data Governance, in accordo con la Policy di Sicurezza Informatica e con le Policy e i processi di Gestione del Rischio informatico, che indirizzano le misure di protezione a fronte dei livelli di classificazione delle informazioni aziendali.
Nel rispetto del Regolamento Europeo sulla privacy, la Data Protection richiede, inoltre, l'osservanza del principio di minimizzazione, al fine di garantire che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

5.1.3 Data Architecture

La Data Architecture indirizza i processi di definizione dell'architettura tecnologica, logica e fisica, a supporto del sistema di gestione del patrimonio informativo della Società, al fine di descrivere opportunamente la basi dati, i flussi informativi e la conseguente collocazione delle informazioni negli archivi aziendali.
I principi di Data Architecture indirizzano i requisiti, i modelli, le politiche, le regole o standard che governano i dati raccolti, oltre a definirne le modalità di utilizzo a livello di sistemi informativi.
In particolare, la Data Architecture indirizza:

- la tassonomia delle informazioni aziendali, sia di Business che IT, con la mappatura dei sistemi applicativi che la implementano;
- l'architettura dei dati che deve garantire la loro coerenza e affidabilità basandosi su un modello in linea con la strategia di Data Governance;

- le politiche per l'utilizzo dei dati e le modalità di replica tra sistemi master e sistemi slave;
- le tecnologie a supporto della gestione dell'architettura logica e fisica delle informazioni aziendali;
- l'opportuna documentazione delle fonti alimentanti, dei flussi di raccolta dati e di relativa elaborazione;
- le politiche di conservazione dei dati le finalità dei trattamenti.

In linea con l'approccio definito dal Modello di data Governance della Capogruppo Banca Mediolanum, i dati aziendali sono rappresentati secondo una categorizzazione proposta dalla Capogruppo, opportunamente adeguata ed integrata alle caratteristiche del business propri del Gruppo.
Elemento centrale del Modello è l'Oggetto Informativo (report, aggregazioni, flussi informativi, applicazioni, basi dati interne ed esterne ecc…) che identifica l'unità informativa elementare utilizzata per rappresentare il patrimonio informativo aziendale.

Tale mappa delle informazioni con vista Business deve essere opportunamente raccordata con la mappa dei dati a livello fisico, in linea con i principi di Data Architecture.

A tal scopo, la disciplina definita come "Data Lineage", in linea con la metodologia adottata dal Gruppo, indirizza le modalità di rappresentazione e valutazione del processo di produzione di un Oggetto Informativo, elemento chiave per la definizione dei controlli di qualità, per la valutazione dei relativi indicatori e attribuzione delle responsabilità.
Il Data Lineage descrive il ciclo di vita del dato nei processi di generazione, trasformazione ed arricchimento per un appropriato governo sul contenuto e la consistenza delle informazioni considerandone l'intero percorso fin dall'origine, ed è propedeutico:

- alla definizione dell'approccio per la mappatura delle informazioni basata su un Glossario di Business e sul Dizionario dei Metadati, al fine di migliorare la comprensione e la conoscenza del patrimonio informativo della Società e favorire l'interazione tra le linee di business e la possibilità di acquisire nuovo valore dai dati;
- al tracciamento delle modalità con le quali le informazioni fluiscono all'interno dei processi e delle applicazioni favorendone la documentazione e la ricostruibilità in relazione alle trasformazioni ed aggregazioni applicate;
- alla descrizione dei processi di generazione, trasformazione ed arricchimento nell'intero ciclo di vita del dato, al fine di governare al meglio i requisiti di qualità dei dati, individuando l'eventuale insorgenza di errori/anomalie fin dall'origine e sull'intero percorso;

- alla conoscenza delle relazioni source-target tra dati fisici lungo la catena di elaborazione, al fine di identificare gli impatti (backward e forward, a monte e a valle) derivanti da inserimenti, cancellazioni, variazioni di campi in tabelle o flussi coinvolti;
- all'identificazione delle relazioni tra dati logici/di business e campi fisici di flussi e tabelle, al fine di supportare efficacemente le comunicazioni tra Business (Data User, Data Owner) e ICT nella gestione delle varie prospettive di Data Governance.

5.2 RUOLI DI DATA GOVERNANCE

Gli organi e le unità organizzative descritte al precedente capitolo 4 definiscono, attuano e monitorano nel tempo la complessiva adeguatezza del Modello di Data Governance.
Tutte le unità organizzative della Società hanno la responsabilità del presidio della Data Governance per gli ambiti di competenza. All'interno di ciascuna struttura organizzativa, inclusa nel perimetro di rilevanza, sono individuate le figure di seguito riportate, relative al processo di gestione dei dati.
L'assegnazione di ruoli e responsabilità specifiche nelle unità organizzative coinvolte è perseguita:

- **senza alterare gli obiettivi delle singole funzioni**: i ruoli e le responsabilità del sistema di gestione dei dati si basano sugli assetti organizzativi della Società evidenziando, ove necessario, le figure attive nel processo di verifica e di governo della qualità del dato;
- **rafforzando il presidio di qualità dei dati**: le figure previste dal sistema di gestione dei dati sono presenti sia a livello di sistema alimentante che di sistema ricevente, lungo tutta la filiera del dato.

5.2.1 Data Owner

Il Data Owner (DO) riveste un ruolo centrale nel Modello di Data Governance in quanto responsabile della gestione, evoluzione e qualità dei dati degli Oggetti Informativi ad esso attribuiti ed è individuato a livello di responsabile di Divisione / Direzione.
Ambiti principali di competenza:

- **Presidio ambiti informativi**: definire gli obiettivi, i requisiti e le modalità di gestione dei dati relativi al proprio perimetro di competenza con il supporto della Perspective Organization & Business Continuity.
- **Definizione dei controlli di qualità**: è responsabile, supportato dalla Perspective Organization & Business Continuity, della definizione del catalogo dei controlli di qualità che identifica sulla base dei requisiti normativi, delle evidenze in termini di controllo e dei risultati dell'attività di analisi dei rischi.

- **Esecuzione dei controlli**: è responsabile, supportato dal Referente Operativo, Control Owner e System Owner, di verificare la corretta esecuzione dei controlli (di linea, andamentali, puntuali e di quadratura) a presidio della qualità dei dati gestiti.
- **Gestione delle anomalie**: congiuntamente al System Owner e al Referente Operativo, ove presente, è responsabile dell'esecuzione degli opportuni approfondimenti sulle anomalie riscontrate per individuare le cause che possono aver generato un eventuale problema di qualità dei dati e indirizzare le opportune attività di remediation delle anomalie riscontrate.
- **Reporting**: è responsabile della formalizzazione dei risultati relativi alla valutazione della qualità dei dati nel proprio perimetro di riferimento rappresentati anche per il tramite degli eventuali indicatori di qualità applicati (Key Quality Indicator).
- **Monitoraggio del processo**: è responsabile del monitoraggio del processo nel proprio perimetro di riferimento. Tale attività è principalmente finalizzata ad assicurare che i dati rientranti nel proprio dominio siano gestiti attraverso l'intero ciclo di vita secondo i processi definiti, individuando evoluzioni ed integrazioni al dominio dei dati di cui è responsabile;
- **Iniziative informatiche:** il Data Owner promuove, di norma con cadenza annuale le opportune iniziative informatiche, verificandone la coerenza con le esigenze di trattamento del dato espresse dalle linee di business e tenuto conto delle strategie aziendali.

5.2.2 Referente Operativo

Il Referente Operativo (RO) è una figura, identificata dal Data Owner con cui in qualche caso può corrispondere, che opera in suo supporto. Può essere delegato dal Data Owner stesso in relazione a specifiche attività o, più frequentemente, al governo della qualità dei dati in relazione a uno o più Oggetti Informativi. In quest'ultimo caso esercita le attività in capo al Data Owner.

5.2.3 Control Owner

Il Control Owner (CO) è responsabile della definizione ed esecuzione dei controlli di qualità dei dati relativi al proprio perimetro di competenza, in accordo con il Data Owner, in particolare:

- definisce i controlli di qualità per assicurare nel continuo e misurare la qualità dei dati, supportato dalla Perspective Organization & Business Continuity;
- è responsabile dell'esecuzione dei controlli funzionali, manuali e/o operativi di propria competenza;

- è responsabile della definizione dei criteri di valutazione degli esiti dei controlli in accordo con il Data Owner e la Perspective Organization & Business Continuity (Key Quality Indicator);
- è responsabile del monitoraggio del processo di controllo nel proprio perimetro di riferimento; tale attività è principalmente finalizzata a verificare il rispetto delle tempistiche di svolgimento delle attività di controllo e l'esito delle stesse.

Il Control Owner può coincidere con il Referente Operativo.

5.2.4 System Owner

Strutture responsabili, da un punto di vista tecnico, delle basi e strutture dati, interne ed esterne, che costituiscono le fonti alimentanti dei dati afferenti a uno specifico ambito informativo. All'interno di ogni struttura sono individuati i referenti - per ogni ambito applicativo/informativo - che assumono il ruolo di System Owner (SO). Il System Owner è responsabile del presidio tecnico e funzionale degli ambiti in perimetro ed è il riferimento tecnico e applicativo del Data Owner.
Le principali responsabilità del System Owner sono:

- eseguire i controlli di tipo tecnico sulle applicazioni in gestione (ricezione/invio flussi, gestione scarti, duplicazione chiavi, etc…);
- implementare i controlli di qualità, secondo le specifiche fornite dal Data Owner;
- risolvere le anomalie tecniche derivanti da segnalazioni in ambito Data Quality;
- realizzare gli interventi di evoluzione e ottimizzazione in relazione alla gestione dei dati sulle applicazioni di propria competenza;
- documentare le applicazioni correttamente;
- attuare i piani di rientro relativamente alla gestione dei sistemi IT;
- applicare i requisiti di sicurezza per quanto concerne il sistema di gestione dei dati in conformità alla normativa interna in materia.

6 Riferimenti Normativi

I principi e le regole definiti nel presente Documento fanno riferimento al seguente contesto legislativo e regolamentare:

- Circolare 285 del 17 Dicembre 2013 di Banca d'Italia "Disposizioni di vigilanza per le banche" e successivi aggiornamenti;
- Disposizioni di Vigilanza per gli Istituti di pagamento e gli Istituti di moneta elettronica - Provvedimento del 17 maggio 2016 e successivi aggiornamenti.