Politica di Privacy, Governance del Dato, Sicurezza delle Informazioni e Controllo Qualità

Obiettivo

Garantire la riservatezza, integrità e disponibilità delle informazioni aziendali), in coerenza con il Sistema di Gestione della Qualità (MSGQ) e con i requisiti ISQM applicabili.

Assicurare l'accuratezza e tracciabilità di dati e informazioni (inclusi quelli utilizzati nel processo di rating ESG).

Proteggere i dati personali, dei clienti, dei dipendenti e dei partner commerciali.

Gestione dei dati in modo lecito, corretto e trasparente.

Responsabili

Ruolo	Responsabilità specifica nell'ambito della politica
Responsabile Sistemi Informativi / IT	Garantisce la sicurezza, la disponibilità e l'integrità dei sistemi e dei dati utilizzati nel processo di rating.
Responsabile SGQ, Risk e ESG	Supervisiona l'applicazione dei controlli di qualità lungo l'intero ciclo di vita del dato e del rating.
Compliance Officer (CO)	Verifica la conformità dei processi di trattamento dati alla normativa privacy e di settore applicabile.

Elementi

Holonic Network identifica e qualifica le fonti, registra la raccolta, verifica completezza, coerenza, accuratezza e tempestività, gestisce dati non pubblici, dati mancanti, proxy e stime, conserva le correzioni e sottopone il dataset a controllo indipendente prima dell'utilizzo nel rating.

HN Finance mantiene controlli sugli accessi, classificazione delle informazioni, informazioni riservate, incidenti, backup, ripristino, continuità operativa, disaster recovery, test periodici e conservazione delle registrazioni.

Gli elementi della politica sono:

- Procedure di validazione e controllo qualità dei dati di input provenienti da fonti esterne (Data Providers) e interne, con tracciabilità delle correzioni effettuate.
- Adozione di misure di sicurezza informatica proporzionate al rischio per la protezione dei dati e dei sistemi utilizzati nei processi aziendali (con particolare attenziona al processo di rating).
- Definizione e attuazione di procedure di prevenzione e gestione tempestiva degli incidenti di sicurezza e di continuità operativa (business continuity / disaster recovery).
- Conservazione documentata di tutte le registrazioni relative al processo di determinazione degli output dei servizi (con particolare attenzione al processo di rating), per un periodo conforme agli obblighi regolamentari.
- Limitazione dell'accesso ai dati sensibili e ai sistemi di rating al solo personale autorizzato, con tracciabilità degli accessi.
- Assicurazione di una raccolta ed un utilizzo dei dati per finalità legittime e limitate allo stretto necessario per l'erogazione dei prodotti e servizi offerti dalla Società.

Indicatori Chiave di Prestazione (KPI)

Indicatore (KPI)	Modalità di calcolo / fonte
N° incidenti di sicurezza informatica rilevati	Registro incidenti IT
N° di violazione dei dati personali	Registro incidenti IT
N° di reclami relativi alla privacy o sicurezza delle informazioni	Registro reclami
N. non conformità rilevate negli internal audit MSGQ	Registro audit interni
Disponibilità dei sistemi informativi (% uptime)	

Riferimenti

Regolamento (UE) 2024/3005: *Art. 23 (qualità delle metodologie); principi ISQM 1 / ISQM 2 / ISQM Italia 1*

Linee Guida OCSE per la Condotta d'Impresa Responsabile (RBC): *Cap. III (Divulgazione e accuratezza delle informazioni); Cap. II (Diligenza dovuta nella gestione dei dati).*