DATA GOVERNANCE E COMPLIANCE INTEGRATA

Il telemarketing come caso applicativo di governo del dato, gestione del rischio e accountability

Dott.ssa Emanuela Ascione
Data Protection Officer W3

Community DPO, CISO e Data Governance -Gruppo di Lavoro Compliance Integrata Unindustria

Roma, 22 giugno 2026

Il telemarketing come processo di Data Governance

Negli ultimi anni il dibattito sul telemarketing è stato prevalentemente incentrato sulle sanzioni privacy.

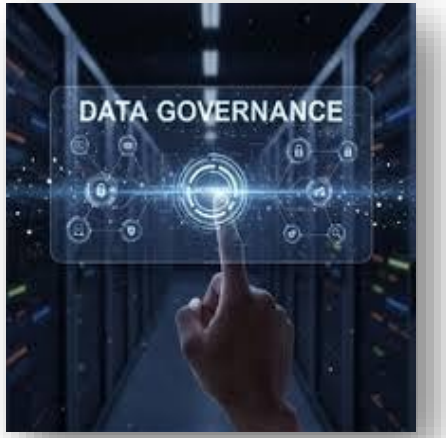
In realtà, **il telemarketing** costituisce un **processo aziendale trasversale** che coinvolge:

- qualità del dato personale
- legittimità del trattamento
- gestione dei consensi
- sicurezza delle informazioni
- monitoraggio dei fornitori
- controllo dei rischi operativi

Pertanto non può essere governato esclusivamente dal DPO ma richiede una **visione integrata** tra i vari dipartimenti aziendali:

- Privacy
- Compliance
- Legal
- Internal Audit
- IT Security
- Business

Il telemarketing rappresenta un esempio concreto di come la qualità della **Data Governance** incida direttamente sulla capacità dell'organizzazione di presidiare rischi, compliance e fiducia del cliente



Il ruolo della Data Governance

Quando parliamo di **Data Governance** non parliamo semplicemente di proteggere il dato.
Il **dato** utilizzato per finalità commerciali deve essere governato lungo tutto il suo ciclo di vita.

Elementi essenziali:

Data lineage - Comprendere
- da dove arriva il dato
- chi lo modifica
- chi lo utilizza
- per quali finalità

Data quality - Garantire
- correttezza
- aggiornamento
- minimizzazione
- conservazione coerente

Accountability - Saper dimostrare
- raccolta del consenso
- gestione delle opposizioni
- esercizio dei diritti dell'interessato

La **tracciabilità del dato** rappresenta oggi un requisito non solo di conformità privacy, ma di governo aziendale e gestione del rischio.

I principali rischi: dove si generano le criticità

Una delle caratteristiche più interessanti del telemarketing è che una singola debolezza può propagarsi rapidamente.

Un dato raccolto male può generare vari rischi:

Rischi Privacy
- Consensi non validi
- Utilizzo improprio dei dati
- Conservazione eccessiva

Rischi Operativi
- Errori di profilazione
- Mancata sincronizzazione delle opposizioni
- Database non aggiornati

Rischi Regolatori
- Provvedimenti del Garante
- Contenziosi
- Sanzioni

Rischi Reputazionali
- Chiamate indesiderate
- Reclami
- Esposizione mediatica

Una debolezza nella governance del dato tende a propagarsi lungo tutta la catena del rischio

Il ruolo dei fornitori

Il rischio si estende oltre il perimetro aziendale

In un **processo di Teleselling** intervengono:

- Contact center
- Agenzie commerciali
- Lead provider
- Società di comparazione
- Subfornitori

Le domande chiave

- Chi tratta il dato?
- Con quali istruzioni?
- Con quali controlli?
- Con quali evidenze?

Nelle organizzazioni complesse la filiera dei fornitori costituisce una componente essenziale del sistema di controllo e resilienza aziendale

Elementi di governance: Codice di Condotta Telemarketing e Teleselling

Elementi di governance

- adesione volontaria a regole condivise di settore
- organismo indipendente di monitoraggio
- verifiche documentali e controlli periodici
- audit sui soggetti della filiera commerciale
- misure correttive e miglioramento continuo

Valore per l'organizzazione

- rafforzamento dei presidi di controllo
- riduzione del rischio operativo
- maggiore affidabilità della filiera
- evidenze di accountability

Codice di Condotta per le Attività di Telemarketing e Teleselling

Sicurezza informatica e resilienza

Collegandosi al punto dell'ordine del giorno dedicato alla cybersecurity e alla Direttiva CER, il telemarketing evidenzia anche aspetti di **resilienza organizzativa**.

Le **principali minacce** riguardano:

- accessi abusivi ai CRM
- esfiltrazione di database clienti
- utilizzo improprio delle credenziali da parte di outsourcer
- frodi commerciali
- campagne di vendita realizzate da soggetti non autorizzati

La **protezione del dato commerciale** è oggi un elemento essenziale della resilienza aziendale

La **resilienza organizzativa** richiede una visione integrata tra protezione del dato, sicurezza delle informazioni e continuità dei processi critici.

Sicurezza informatica e resilienza

Le imprese stanno assistendo a una **crescente convergenza normativa** tra:

- GDPR;
- NIS2;
- Data Act;
- AI Act;
- Direttiva CER;
- normativa consumeristica.

- ❑ **Stessi dati**
- ❑ **Stessi processi**
- ❑ **Rischi differenti**

Ciò impone modelli organizzativi che evitino la gestione a silos della compliance.
Il telemarketing è uno degli ambiti in cui questa convergenza emerge con maggiore evidenza

Una filiera commerciale non governata può diventare un fattore di vulnerabilità organizzativa

Conclusioni

L'esperienza maturata nel settore Telco dimostra che il telemarketing non deve essere considerato esclusivamente un tema data protection.

È piuttosto un **laboratorio di Data Governance e Compliance Integrata** in cui convergono:

- protezione dei dati
- sicurezza informatica
- controllo dei fornitori
- gestione del rischio
- accountability
- tutela della reputazione aziendale

La vera sfida per le imprese non è soltanto rispettare gli obblighi normativi, ma **costruire un modello di governance capace di coniugare innovazione commerciale**, **fiducia del cliente e sostenibilità regolatoria**.

La crescente convergenza tra **GDPR, NIS2 e CER** evidenzia come la protezione del dato, il governo dei fornitori e la resilienza dei processi rappresentino oggi elementi inscindibili di una moderna governance aziendale

Grazie per l'attenzione