POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E LA PROTEZIONE DEI DATI PERSONALI

(ISO/IEC 27001 + ISO/IEC 27701)
SWG S.p.A.

Sommario

1. Introduzione

SWG S.p.A. Società Benefit (di seguito “SWG”) riconosce che le informazioni, inclusi i dati personali raccolti nell’ambito delle attività di ricerca e sondaggi, rappresentano un asset strategico fondamentale per il proprio business.

In particolare, l’attività di:

- raccolta ed elaborazione di opinioni,
- analisi di dati statistici,
- gestione di panel e campagne di ricerca,

implica il trattamento di **grandi volumi di dati, spesso personali e potenzialmente sensibili**, con rischi elevati per i diritti degli interessati.

Pertanto, SWG si impegna a:

- garantire la **riservatezza, integrità e disponibilità delle informazioni**,
- assicurare la **protezione dei dati personali (PII)** lungo tutto il ciclo di vita,
- adottare un approccio basato sul rischio e sulla responsabilizzazione (accountability).

Questa Politica definisce i principi guida del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI/ISMS) e del Sistema di Gestione delle Informazioni sulla Privacy (PIMS).

2. Riferimenti normativi

La presente Politica si basa sulle seguenti norme:

- UNI CEI EN ISO/IEC 27001:2024 – Sistemi di gestione per la sicurezza delle informazioni
- UNI CEI EN ISO/IEC 27002:2023 – Controlli di sicurezza delle informazioni
- UNI CEI EN ISO/IEC 27701:2025 – Sistemi di gestione delle informazioni sulla privacy
- Regolamento (UE) 2016/679 – GDPR
- Codice Privacy (D.lgs. 196/2003 e s.m.i.)

3. Impegno della Direzione

La Direzione di SWG:

- approva e sostiene il SGSI e il PIMS;
- assicura che la sicurezza delle informazioni sia **integrata nei processi aziendali**;
- garantisce la disponibilità di risorse adeguate;
- promuove una cultura della sicurezza e della protezione dei dati;
- definisce obiettivi misurabili e ne monitora il raggiungimento;
- assegna ruoli e responsabilità chiare;
- si impegna al miglioramento continuo del sistema.

La Direzione riconosce inoltre che l’adozione di un SGSI è una decisione strategica influenzata da rischi, obiettivi e contesto.

4. Campo di applicazione

Il Sistema di Gestione per la Sicurezza delle Informazioni e la Privacy di SWG si applica al seguente perimetro:

“Progettazione ed esecuzione di sondaggi di opinione e ricerche di mercato quantitative e qualitative. Esecuzione di fieldwork qualitativo e quantitativo telefonico, on line, face to face e mistery.”

Lo scopo include:

- sistemi informativi e piattaforme di raccolta dati (web, CATI, CAPI, panel);
- basi dati e archivi di ricerca;
- processi di analisi statistica e reporting;
- fornitori e partner coinvolti nel fieldwork;
- personale interno ed esterno.

Lo scopo considera:

- informazioni aziendali,
- dati dei clienti,
- dati personali dei rispondenti (inclusi dati di profilazione),
- metadati e informazioni tecniche.

5. Politica per la sicurezza delle informazioni e la privacy

5.1 Principi generali

SWG adotta i seguenti principi:

- **Approccio basato sul rischio**: identificazione, valutazione e trattamento dei rischi per sicurezza e privacy
- **Protezione by design e by default**
- **Accountability e dimostrabilità** (GDPR)
- **Minimizzazione del dato e limitazione delle finalità**
- **Continuità operativa e resilienza**

5.2 Sicurezza delle informazioni

SWG garantisce:

- protezione della **riservatezza** (accesso solo autorizzato)
- tutela dell’**integrità** (dati corretti e non alterati)
- disponibilità delle informazioni e dei sistemi

attraverso:

- controlli tecnici e organizzativi,
- gestione degli accessi,
- cifratura, anonimizzazione e pseudonimizzazione,
- protezione delle infrastrutture e dei dispositivi.

Tali misure sono definite in funzione del rischio e riesaminate periodicamente.

5.3 Protezione dei dati personali

SWG si impegna a:

- trattare dati personali in modo **lecito, corretto e trasparente**
- raccogliere dati solo per **finalità determinate e legittime**
- limitare i dati a quanto necessario (**data minimization**)
- garantire sicurezza e riservatezza dei dati personali
- rispettare i diritti degli interessati (accesso, rettifica, cancellazione, opposizione, ecc.)

Inoltre, SWG:

- definisce chiaramente i ruoli (titolare/responsabile),
- mantiene il registro dei trattamenti,
- effettua DPIA per trattamenti a rischio elevato,
- gestisce data breach secondo procedure definite.

5.4 Gestione dei fornitori e del fieldwork

Considerata la natura del business (intervistatori, panel provider, outsourcing):
SWG richiede che:

- i fornitori rispettino requisiti di sicurezza e privacy equivalenti,
- siano sottoposti a valutazione e monitoraggio,
- siano vincolati contrattualmente (es. NDA, DPA).

5.5 Formazione e consapevolezza

SWG garantisce che tutto il personale:

- sia formato sui principi di sicurezza e privacy,
- comprenda i rischi specifici del settore (profilazione, anonimizzazione, bias),
- conosca le procedure operative.

5.6 Gestione degli incidenti

SWG implementa processi per:

- rilevare e segnalare incidenti di sicurezza,
- gestire violazioni di dati personali (data breach),
- notificare alle autorità e agli interessati quando necessario.

5.7 Miglioramento continuo

Il SGSI/PIMS è soggetto a:

- audit interni,
- riesame della Direzione,
- monitoraggio delle performance,
- aggiornamento continuo.