MISURE DI CYBERSECURITY E DATA PROTECTION

Il presente Allegato descrive, in forma sintetica ma sostanziale, le principali misure tecniche, organizzative e procedurali adottate da **Demos Marketing International S.r.l.** per garantire un livello adeguato di sicurezza nel trattamento dei dati personali, in coerenza con il Regolamento (UE) 2016/679 ("GDPR"), con i principi di responsabilizzazione, privacy by design e by default e con le esigenze di riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento.

Le misure qui descritte si applicano ai trattamenti svolti da Demos nell'ambito delle proprie attività di ricerca, analisi e gestione del Panel, sia quando la Società opera in qualità di **Titolare del trattamento**, sia quando opera in qualità di **Responsabile del trattamento** per conto di propri Clienti o Committenti, nei limiti e secondo il ruolo concretamente ricoperto nel singolo progetto.

Per ragioni di sicurezza, il presente Allegato ha natura descrittiva generale e non riporta in forma analitica l'intera configurazione tecnica, le specifiche architetturali, i parametri di difesa, i dettagli infrastrutturali o altri elementi la cui divulgazione pubblica potrebbe ridurre l'efficacia dei presidi adottati.

1. Modello organizzativo di protezione dei dati

Demos ha adottato un sistema organizzativo volto a garantire la conformità dei trattamenti ai principi e agli obblighi previsti dalla normativa in materia di protezione dei dati personali. Tale assetto comprende, tra l'altro:

- la definizione di ruoli, responsabilità e livelli autorizzativi;
- la tenuta e l'aggiornamento della documentazione privacy rilevante;
- la gestione dei rapporti contrattuali con responsabili e sub-responsabili del trattamento;
- la formalizzazione delle istruzioni al personale autorizzato;
- la previsione di procedure per l'esercizio dei diritti degli interessati;
- la gestione delle verifiche, dei controlli e delle eventuali azioni correttive.

La Società adotta inoltre un approccio basato sul rischio, orientato alla valutazione preventiva dell'impatto organizzativo e tecnico dei trattamenti, alla minimizzazione dei dati e alla verifica periodica dell'adeguatezza delle misure implementate.

2. Misure di riservatezza e controllo degli accessi

Demos adotta misure finalizzate a impedire accessi fisici e logici non autorizzati ai dati personali, ai locali, ai sistemi, alle piattaforme e agli archivi nei quali i dati sono trattati o conservati.

Tali misure comprendono, in funzione della natura dei sistemi e dei trattamenti:

- controllo degli accessi ai locali e alle aree riservate;
- sistemi di chiusura, identificazione e regolazione degli ingressi;
- procedure di registrazione e gestione dei visitatori e del personale esterno;
- assegnazione individuale delle credenziali di accesso;
- policy di autenticazione sicura e di gestione delle password;
- procedure di disabilitazione, revoca o revisione tempestiva degli account non più necessari;

- tracciamento e monitoraggio degli accessi ai sistemi e alle applicazioni.

L'accesso ai dati e agli strumenti di trattamento è consentito esclusivamente ai soggetti autorizzati, nei limiti delle mansioni svolte e secondo il principio di **necessità, pertinenza e minimo privilegio**. Ove appropriato rispetto al rischio e alla tipologia di sistema, la Società adotta anche sistemi di autenticazione rafforzata e misure aggiuntive di protezione degli accessi privilegiati.

3. Profili autorizzativi e segregazione degli accessi

La Società definisce e applica profili di autorizzazione differenziati, calibrati in relazione al ruolo ricoperto, alle mansioni concretamente svolte e alla necessità di accesso ai dati.

Le autorizzazioni sono attribuite, modificate e revocate mediante procedure formalizzate e soggette a riesame periodico. Gli accessi amministrativi e i privilegi elevati sono gestiti con particolare cautela e, ove previsti, sono attribuiti in modo individuale, limitato, tracciabile e verificabile.

Sono inoltre adottate misure organizzative e tecniche volte a:

- limitare la consultazione, modifica, esportazione o cancellazione dei dati ai soli soggetti abilitati;
- registrare gli accessi e gli eventi rilevanti di sistema;
- controllare le attività tecniche svolte da amministratori di sistema o da personale esterno autorizzato;
- assicurare la distruzione sicura dei supporti di memorizzazione e dei documenti cartacei non più necessari.

4. Pseudonimizzazione, cifratura e protezione dei dati

Demos adotta, ove appropriate rispetto al rischio e alla natura dei trattamenti, misure di protezione ulteriori quali la **pseudonimizzazione**, la **separazione dei dati identificativi**, la **cifratura dei dati a riposo e in transito**, la protezione dei backup e la limitazione dell'accessibilità ai soli soggetti autorizzati.

In particolare, la Società tende a distinguere, per quanto possibile, i dati identificativi dai dati di ricerca, dai dati statistici o dai dataset operativi, limitando il collegamento tra tali insiemi ai soli casi in cui esso sia effettivamente necessario per esigenze di gestione, controllo qualità, adempimenti amministrativi o tutela dei diritti.

Sono inoltre adottate politiche di gestione sicura delle chiavi di cifratura, dei supporti rimovibili, dei dispositivi mobili e degli strumenti utilizzati per il trattamento, in modo da ridurre il rischio di accessi indebiti, perdita, sottrazione o uso non autorizzato dei dati. L'art. 32 GDPR richiama espressamente, tra le misure possibili, pseudonimizzazione e cifratura dei dati personali.

5. Sicurezza della trasmissione dei dati

La trasmissione dei dati personali tra sistemi, sedi, piattaforme, postazioni operative o soggetti autorizzati avviene mediante canali e modalità idonei a garantirne la sicurezza, la riservatezza e l'integrità.

A tal fine, Demos adotta misure quali, a seconda dei contesti applicativi:

- utilizzo di protocolli sicuri e cifrati;
- protezione dei canali di accesso remoto;
- adozione di soluzioni sicure per la condivisione di file e documenti;
- cifratura di allegati o documenti contenenti dati personali;
- trasmissione separata delle credenziali o delle password di protezione;
- uso di elenchi di destinatari autorizzati e di istruzioni operative per la corretta circolazione dei dati.

Qualora la comunicazione o il trasferimento di dati avvenga verso terzi autorizzati, tali flussi sono disciplinati secondo il ruolo privacy ricoperto dai soggetti coinvolti e secondo idonee misure contrattuali e organizzative.

6. Integrità, esattezza e aggiornamento dei dati

La Società adotta misure volte a garantire che i dati personali trattati siano esatti, aggiornati, coerenti con le finalità perseguite e non alterati indebitamente.

A tal fine sono previste, tra l'altro:

- procedure di validazione e verifica dei dati inseriti;
- controlli di coerenza nei sistemi e nelle applicazioni;
- logiche di tracciabilità delle modifiche rilevanti;
- procedure per la rettifica, l'aggiornamento o la cancellazione dei dati inesatti, obsoleti o non più necessari;
- regole di conservazione e cancellazione coerenti con le finalità del trattamento.

Tali misure contribuiscono a dare attuazione ai principi di esattezza e limitazione della conservazione previsti dal GDPR.

7. Disponibilità, continuità operativa e resilienza

Demos adotta misure tecniche e organizzative finalizzate a garantire la disponibilità dei dati, la continuità dei servizi essenziali e la capacità di ripristinare in tempi ragionevoli la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico.

Tali misure comprendono, in funzione dei sistemi e dei contesti operativi:

- procedure di backup periodico e protetto;
- piani di ripristino e recovery;
- verifiche e test periodici di ripristino;
- misure di protezione ambientale e infrastrutturale;
- monitoraggio dei sistemi, delle anomalie e degli eventi rilevanti;
- presidi di continuità operativa e, ove applicabile, di Disaster Recovery.

L'art. 32 GDPR richiama espressamente anche la capacità di assicurare su base permanente riservatezza, integrità, disponibilità e resilienza dei sistemi, nonché di ripristinare tempestivamente disponibilità e accesso ai dati in caso di incidente.

8. Protezione della rete, dei dispositivi e del software

La Società adotta misure di protezione della rete, dei dispositivi, dei server, degli endpoint, delle piattaforme e del software utilizzato per il trattamento dei dati, sulla base degli standard tecnici generalmente riconosciuti e in coerenza con il rischio.

Rientrano tra tali presidi, a titolo esemplificativo:

- strumenti di filtraggio e segmentazione del traffico di rete;
- sistemi di rilevazione, prevenzione e monitoraggio degli eventi di sicurezza;
- protezioni anti malware e anti-intrusione;
- controllo delle configurazioni;
- gestione degli aggiornamenti di sicurezza e delle patch;
- attività periodiche di assesment e verifica delle vulnerabilità;
- inventario e monitoraggio delle risorse informatiche e dei software autorizzati.

Le risorse IT e i software sono oggetto di gestione attiva, monitoraggio, aggiornamento e controllo, al fine di ridurre il rischio connesso a configurazioni non autorizzate, obsolescenza tecnologica o vulnerabilità note.

9. Gestione degli incidenti di sicurezza e dei data breach

Demos ha adottato procedure organizzative per la rilevazione, la gestione, la valutazione e la registrazione degli incidenti di sicurezza e delle eventuali violazioni dei dati personali.

Tali procedure prevedono, tra l'altro:

- canali di segnalazione interna;
- ruoli e responsabilità per la valutazione degli incidenti;
- criteri di classificazione e gestione degli eventi;
- registrazione e documentazione degli incidenti rilevanti;
- meccanismi di coordinamento con il Titolare del trattamento, ove Demos operi quale Responsabile;
- procedure per la notifica delle violazioni e per le ulteriori misure richieste dalla normativa applicabile.

Gli articoli 33 e 34 GDPR disciplinano rispettivamente la notifica della violazione all'autorità di controllo e, nei casi previsti, la comunicazione della violazione agli interessati.

10. Privacy by design e by default

Nella progettazione e nell'evoluzione dei processi, dei flussi informativi, delle piattaforme e degli strumenti di trattamento, Demos adotta un approccio ispirato ai principi di **protezione dei dati fin dalla progettazione** e **per impostazione predefinita**.

Ciò comporta, in particolare:

- valutazione preventiva delle finalità e dei flussi di trattamento;
- minimizzazione dei dati raccolti, utilizzati, comunicati e conservati;
- limitazione degli accessi e delle funzionalità non necessarie;
- attenzione alle caratteristiche di sicurezza dei software e dei servizi adottati;
- verifica dell'opportunità di ricorrere a pseudonimizzazione, segregazione logica o ulteriori cautele di protezione.

L'art. 25 GDPR richiede espressamente l'adozione di misure tecniche e organizzative adeguate per attuare i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita.

11. Formazione, riservatezza e controllo sui fornitori

Il personale autorizzato al trattamento riceve istruzioni adeguate in materia di protezione dei dati personali, sicurezza delle informazioni, corretto utilizzo degli strumenti aziendali e gestione delle anomalie o degli incidenti.

La Società adotta inoltre:

- impegni di riservatezza e obblighi di confidenzialità;
- procedure di autorizzazione e istruzione del personale;
- criteri di selezione, qualifica e controllo dei fornitori che trattano dati per conto della Società;
- accordi contrattuali con responsabili e sub-responsabili del trattamento, ove necessari.

L'art. 28 GDPR richiede che il ricorso a un responsabile del trattamento avvenga tramite soggetti che presentino garanzie sufficienti e mediante un contratto o altro atto giuridico che disciplini il trattamento per conto del titolare.

12. Verifiche periodiche, audit e miglioramento continuo

Le misure di sicurezza e protezione dei dati non sono considerate statiche, ma oggetto di verifica periodica, riesame, aggiornamento e miglioramento continuo.

La Società prevede, in funzione della propria organizzazione e dei trattamenti svolti:

- controlli periodici sull'adeguatezza delle misure tecniche e organizzative;
- audit interni o di seconda parte;
- verifiche documentate sui processi di trattamento;
- riesami organizzativi e aggiornamenti delle policy;
- eventuali assesment o audit di terza parte nell'ambito di percorsi di conformità, qualificazione o certificazione.

Questo approccio è coerente con il principio di accountability e con il requisito di testare, verificare e valutare regolarmente l'efficacia delle misure di sicurezza del trattamento.

13. Standard professionali e impegni di settore

Nello svolgimento delle proprie attività, Demos adotta presidi organizzativi coerenti con i principi di correttezza professionale, qualità del dato, sicurezza delle informazioni, riservatezza e tutela degli interessati propri del settore del market, opinion and social Research.

In tale contesto, la Società opera in coerenza con i principi del **Codice ICC/ESOMAR** applicabile alle attività di ricerca e data analytics e con gli standard organizzativi di settore rilevanti per le attività di ricerca e gestione della qualità. Il Codice ICC/ESOMAR 2025 si applica alle attività di market, opinion and social Research e data analytics; **ISO 20252:2019** disciplina invece i requisiti di servizio per tali attività e precisa che il Directa marketing è fuori dal suo perimetro.

Eventuali riferimenti a certificazioni o percorsi di certificazione in materia di sicurezza delle informazioni o privacy information management saranno comunicati dalla Società esclusivamente nei casi in cui risultino effettivamente conseguiti o formalmente in corso secondo i presupposti documentabili. **ISO/IEC 27001:2022** definisce i requisiti di un sistema di gestione della sicurezza delle informazioni; la serie 27701 resta il riferimento specifico per i sistemi di gestione delle informazioni sulla privacy.

14. Clausola finale

Le misure descritte nel presente Allegato sono adottate secondo un criterio di adeguatezza, proporzionalità, evoluzione tecnologica e valutazione del rischio, e possono essere periodicamente aggiornate, rafforzate o integrate in funzione di modifiche normative, organizzative, tecnologiche o dei trattamenti concretamente svolti.

La versione aggiornata sarà resa disponibile su questa pagina con indicazione della data di ultimo aggiornamento.

Data ultimo aggiornamento: 20 aprile 2026

Dichiaro di aver letto e accettato le misure di Cybersecurity e Data Protection.