theorema
IDEE - VALORI - INNOVAZIONE

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E DATI PERSONALI

Theorema Srl
Viale Tiziano, 80 – 00196 Roma
Tel. 0680687860 r.a. - e-mail: theorema@theorema.it – pec: theorema@pec.theoremasrl.eu
REA. 630802 - P.IVA 01880661002 – C.F. 07825960581 – Capitale Sociale € 210.400,00

1 OGGETTO DEL DOCUMENTO

Theorema, nel fornire servizi di Consulenza di Direzione, si pone come partner professionale dei propri Clienti: uno stile consulenziale che prevede il coinvolgimento diretto nell'analisi delle problematiche, nella ricerca delle soluzioni ed implementazione delle stesse. Theorema si avvale di un know-how specifico e di alto livello, costantemente aggiornato e potenziato, e sviluppa progetti che integrando differenti modalità di intervento – formazione, consulenza, assistenza – garantiscono la creazione di valore tangibile e duraturo.

2 RIFERIMENTI NORMATIVI

- Tecnologia dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni [ISO/IEC 27001]
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [General Data Protection Regulation o GDPR]

3 SCOPO E FINALITÀ

Il presente documento definisce gli obiettivi e gli impegni di Theorema nella gestione della sicurezza, della protezione delle informazioni e dei dati personali e della continuità operativa in conformità con gli standard ISO 27001 e con il Regolamento UE 679/2016.

4 AMBITO DI APPLICAZIONE

Il presente documento è parte integrante del Sistema di Gestione integrato (sicurezza delle informazioni e protezione dei dati personali) implementato nonché degli accordi contrattuali in essere con i propri collaboratori e con le organizzazioni esterne (Clienti, Fornitori, Partner) con le quali intrattiene rapporti economici e/o di collaborazione. Di conseguenza, per "destinatari" o "interessati" si intendono qui compresi:

a) soci, amministratori, dipendenti/collaboratori e professionisti facenti parte della propria Organizzazione
b) persone fisiche di cui Theorema acquisisce direttamente i dati personali nell'ambito della propria attività istituzionale o promozionale
c) esponenti di organizzazioni terze (clienti, business partner, fornitori...) e persone fisiche di cui questi soggetti detengano dati personali, che collaborino o affidino a Theorema la gestione di attività professionali

La Politica per la sicurezza delle informazioni e dei dati personali di Theorema è messa a disposizione di tutti gli stakeholder rilevanti mediante pubblicazione sul proprio sito istituzionale.

5 OBIETTIVI SPECIFICI DEL SISTEMA DI GESTIONE INTEGRATO SICUREZZA DELLE INFORMAZIONI E PRIVACY

Gli obiettivi del Sistema di Gestione integrato e della presente Politica sono i seguenti:

- allineare tutti i processi aziendali che comportano trattamenti di dati personali o di informazioni rilevanti ai principi stabiliti dall'art. 5 del GDPR nonché a quelli di governance della sicurezza delle informazioni;
- documentare tutti gli adempimenti in materia di protezione dei dati personali e di sicurezza delle informazioni per essere in grado di dimostrare la propria postura di conformità e di sicurezza;
- proteggere i dati personali e le altre informazioni rilevanti trattati dall'organizzazione da accessi non autorizzati, distruzione, perdita o divulgazione accidentale;
- garantire la trasparenza nei trattamenti, assicurando che gli interessati siano pienamente informati sui loro diritti e sui processi di gestione dei dati personali, agevolando e assicurando l'esercizio dei loro diritti;
- salvaguardare la sicurezza delle reti e dei sistemi essenziali per la continuità operativa e la resilienza dell'organizzazione;
- implementare un processo continuo di valutazione e gestione dei rischi informatici finalizzato al miglioramento continuo;
- assicurare una risposta tempestiva ed efficace agli incidenti di sicurezza e una collaborazione attiva con le autorità competenti.

6 GLI IMPEGNI DI THEOREMA

Da sempre impegnata nel rispetto delle leggi e nella prevenzione delle problematiche relative al trattamento delle informazioni e dei dati personali Theorema, con il presente documento, intende formalizzare un quadro di riferimento, rivolto a tutti i soggetti precedentemente individuati per fornire adeguate garanzie in merito ed in particolare si impegna a:

a) rispettare la normativa vigente, i requisiti contrattuali o volontari in materia, garantendo un approccio integrato e proattivo alla protezione dei dati e alla sicurezza delle informazioni;
b) definire le responsabilità, i ruoli ed i compiti a tutti i livelli interni, considerando adeguatamente - nel proprio processo di allocazione del budget - gli investimenti che contribuiscano alla riduzione del rischio sia per la Società che per gli interessati e altri Stakeholder;
c) proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati personali secondo i principi della privacy & security by design e by default;
d) non limitarsi all'adozione di adeguate misure tecniche ma implementare processi e controlli (tecnologici ed organizzativi) che consentano di testare, verificare e valutare regolarmente

l'efficacia delle misure adottate, affinché siano sempre allineate allo stato dell'arte ed alle nuove minacce che si presentino

e) promuovere la consapevolezza e la responsabilizzazione del proprio personale riguardo alla sicurezza informatica e al trattamento dei dati personali, anche attraverso adeguati percorsi formativi;

f) gestire la catena di fornitura, adottando modalità di selezione e valutazione dei partner (anche con riguardo alla sicurezza delle informazioni e dei dati personali) adeguate in funzione del rischio di contesto e dei singoli progetti;

g) incrementare la soddisfazione dei clienti e la brand reputation attraverso l'efficace applicazione degli impegni assunti, promuovendo il miglioramento continuo e complessivo delle proprie modalità gestionali, costantemente riesaminate ai più alti livelli di responsabilità.

6 LE GARANZIE NEI CONFRONTI DEI TITOLARI COMMITTENTI

Theorema Srl:

- non è mai incorsa nella comminazione di condanne in materia di trattamento di dati personali, ad es. con riferimento:
  - ✓ ad uno o più dei reati previsti dal D.lgs. 196/2003 (artt. 167 e ss.) o dall'art. 24-*bis* del D.lgs. 231/2001 in relazione agli apicali dell'Ente o direttamente in capo all'Ente (sanzioni amministrative dipendenti da reato)
  - ✓ alle sanzioni amministrative pecuniarie previste prima dal D.lgs. 196/2003 (artt. 161 e ss.) e successivamente dal GDPR (art. 83)
- non ha mai subito una violazione di dati personali - così come qualificata dall'art. 33 GDPR e dai Motivi 85, 86 e 87 dello stesso Regolamento - che abbia comportano un rischio per gli interessati
- ha implementato il proprio Sistema di Gestione integrato (Sicurezza delle informazioni, ai sensi dello standard ISO 27001 e Privacy, ai sensi del GDPR e normativa correlata)

Ai sensi dell'art. 29 del GDPR e art. 2-*quaterdecies* del D.lgs. 196/2003 e del requisito 5.2 dello standard ISO 27001, ferma restando la titolarità del trattamento in capo alla persona giuridica, Theorema ha affidato l'esercizio delle funzioni gestorie in materia di data protection e sicurezza delle informazioni agli amministratori delegati, ciascuno in riferimento ai processi/progetti ed alle funzioni di supporto interno di competenza; le autorizzazioni al trattamento dei dati sono incorporate negli incarichi professionali formalizzati con i consulenti; per i dipendenti, è formalizzata una specifica autorizzazione al trattamento dei dati, con impegni alla riservatezza ed obblighi in materia di sicurezza delle informazioni che rimangono validi anche dopo la cessazione del rapporto.

Seppur non obbligatorio sulla base del contesto in relazione alle previsioni di cui all'art. 30 GDPR, Theorema ha adottato il registro dei trattamenti in qualità di Titolare (art. 30, par. 1) ed in qualità di Responsabile (art. 30, par. 2) quale strumento utile per il censimento, analisi ed assunzione di consapevolezza sui trattamenti gestiti; il registro contiene anche un'analisi preliminare di impatto dei diversi trattamenti sui diritti e libertà degli interessati.

Le istruzioni ai soggetti autorizzati sono rilasciate:

- attraverso la realizzazione di specifici percorsi formativi periodici interni
- la formalizzazione di procedure, linee guida ed istruzioni

Theorema garantisce l'adozione delle misure di sicurezza di natura tecnologica, organizzativa e procedurale richieste dallo standard ISO 27001, dal GDPR e dalle normative specifiche in ambito cybersecurity obbligatorie per legge o imposte a livello contrattuale. Tali misure sono censite e descritte:

a) nella SOA (Statement of Applicability), sulla base dei requisiti ISO 27001
b) nel Modulo di Implementazione di cui alla Circolare AgID n. 2 del 18/04/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni", in particolare per Committenti del settore pubblico

Nei progetti che comportino la progettazione (preliminare/esecutiva) e lo sviluppo di sistemi informativi custom, Theorema adotta metodologie e standard in grado di garantire i principi di privacy & security by design e by default.

Salvo ove diversamente indicato dal Titolare committente quale istruzione documentata, Theorema conserva i documenti di progetto per un periodo di 10 anni a far data dalla conclusione degli stessi (termine di prescrizione civilistico ordinario), al fine di garantirsi a fronte di eventuali contestazioni di natura contrattuale.

Nell'ambito delle procedure di monitoraggio e riesame del Sistema di Gestione integrato, l'Alta direzione effettua (anche ai sensi dell'art. 32, par. 1, lett. d del GDPR) la verifica delle performance del Sistema; il riesame è svolto congiuntamente dall'Alta direzione con il Privacy Manager e il Responsabile del Sistema di Gestione della Sicurezza delle Informazioni di Theorema.

Theorema infine – nell'eventuale assenza di istruzioni documentate formalizzate dal Titolare committente anche per il tramite di apposito accordo sul trattamento di cui all'art. 28 GDPR - garantisce by default il rispetto delle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento di cui alla Decisione di Esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021.

7 LE GARANZIE NEI CONFRONTI DEGLI INTERESSATI

Oltre all'adozione di adeguate misure di sicurezza tecniche ed organizzative precedentemente riassunte, Theorema garantisce la massima trasparenza nei confronti degli interessati ove operi in qualità di Titolare o contitolare del trattamento, in particolare attraverso:

- il rilascio delle proprie informative (per categoria di stakeholder) richieste dagli artt. 13 e 14 del GDPR in fase di acquisizione dei dati personali, anche messe a disposizione nella sezione "Compliance e Sostenibilità" del proprio sito istituzionale;
- una attenta gestione dei loro diritti, secondo la specifica procedura adottata; il documento fornisce le istruzioni relative al processo di ricezione, gestione ed evasione delle eventuali richieste da parte degli interessati aventi ad oggetto l'esercizio dei diritti sanciti dal GDPR, ricevute sia in qualità di Titolare (o contitolare) del trattamento, ai sensi dell'art. 4 par. 1 n.7 del GDPR, sia in qualità di Responsabile del trattamento ai sensi dell'art. 28 del GDPR.

8 SEGNALAZIONE DI INCIDENTI, EVENTI DI SICUREZZA E RECLAMI

Theorema incoraggia le segnalazioni di ogni problematica, criticità, violazione o non conformità relativa al trattamento di dati personali ed alla sicurezza delle informazioni mediante canali e modalità dedicate che, pur sempre in ossequio alla tutela della reputazione e dell'immagine della Società permettano, da un lato, di svolgere indagini e approfondimenti al fine di valutarne la fondatezza e dall'altro di tutelare la riservatezza del segnalante e del segnalato, anche da qualsivoglia forma di ritorsione.

Le segnalazioni, richieste o reclami, provenienti da qualsivoglia stakeholder interno o esterno, possono essere inviate mediante e-mail al seguente indirizzo: segnalazioni@theorema.it; ogni comunicazione pervenuta sarà gestita nel rispetto dei principi di riservatezza e confidenzialità delle informazioni.

Roma, 22 maggio 2025 **Il Presidente**