POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E DATI PERSONALI

Theorema Srl
Viale Tiziano, 80 – 00196 Roma
Tel. 0680687860 r.a. - Fax 0680687662 - e-mail: theorema@theorema.it – pec: theorema@pec.theoremasrl.eu
REA. 630802 - P.IVA 01880661002 – C.F. 07825960581 – Capitale Sociale € 10.400,00 i.v.

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.

Da sempre impegnata nel rispetto delle leggi e nella prevenzione delle problematiche relative al trattamento dei dati personali affidati dai propri Committenti e più in generale relativi ai propri stakeholder (interni ed esterni), Theorema intende con il presente documento formalizzare un quadro di riferimento, rivolto a tutti i soggetti precedentemente individuati per fornire adeguate garanzie in merito:

a) alla propria capacità, per competenza, esperienza e prassi consolidate adottate, di assicurare il rispetto della normativa vigente in materia di protezione dei dati e degli interessati nonché degli ulteriori requisiti o istruzioni specifiche di volta in volta definiti contrattualmente

b) alla possibilità ed agli strumenti attivati per consentire agli interessati l'esercizio dei diritti che la normativa vigente nel tempo gli riconosce

Il presente documento è parte integrante del Sistema di Gestione della Qualità 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 e professionisti direttamente utilizzati da Theorema nell'esercizio della propria mission societaria

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, all'indirizzo https://www.theorema.it/informazioni-societarie/.

Gli impegni di Theorema

Nella gestione delle proprie attività istituzionali, Theorema si impegna a:

- ✓ avere una visione centrale della sicurezza aziendale e dei dati ed informazioni detenute, secondo i principi della privacy & security by design e by default
- ✓ di conseguenza, considerare adeguatamente nel proprio processo di allocazione del budget gli investimenti che contribuiscano alla riduzione del rischio sia per la Società che per gli interessati
- ✓ non limitarsi all'adozione di adeguate misure tecniche ma implementare anche processi e controlli 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;
- ✓ incrementare la soddisfazione dei clienti e la brand reputation attraverso l'efficace applicazione degli impegni di cui ai punti precedenti, promuovendo il miglioramento continuo e complessivo delle proprie modalità gestionali

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. 24bis 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 certificato il proprio Sistema di Gestione della Qualità ai sensi della ISO 9001:2015 anche per la fornitura di servizi in materia di "*gestione degli adempimenti privacy*"; nell'ambito del sistema certificato, in aderenza ai requisiti organizzativi, gestionali e tecnici di cui al GDPR, Theorema gestisce le misure organizzative, gestionali e tecniche di cui alla normativa richiamata come di seguito descritto.

Ai sensi dell'art. 29 del GDPR e art. 2-quaterdecies del D.Lgs. 196/2003, ferma restando la titolarità del trattamento in capo alla persona giuridica, Theorema ha affidato l'esercizio delle funzioni gestorie in materia di data protection 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.

Seppur non obbligatorio per organizzazioni con meno di 250 dipendenti (art. 30, par. 5 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 gestionali, integrate nel Sistema Qualità certificato; tra queste, Theorema ha approvato la propria procedura di gestione dei data breach (7.5.5-IST-02), che regolamenta le attività interne relative al processo di rilevazione, triage e gestione degli incidenti di sicurezza riguardanti i trattamenti di dati personali svolti, sia in qualità di Titolare 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); in quest'ultimo caso, la procedura garantisce quale SLA nei confronti del Titolare che la comunicazione di cui all'art. 33 par. 2 del GDPR avvenga "*non oltre i termini di notifica eventualmente previsti nell'accordo sul trattamento ex art. 28 sottoscritto con Titolare*"

Theorema garantisce l'adozione delle misure di sicurezza di natura tecnologica, organizzativa e procedurale definite dalla Circolare AgID n. 2 del 18/04/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni". Com'è noto, la circolare di per sé non è vincolante per le società private; Theorema ha però deciso di adottare la metodologia AdID quale standard di riferimento per la verifica di adeguatezza e per l'attestazione delle misure adottate sulla base delle seguenti considerazioni: a) i requisiti (controlli) previsti dalla circolare AgiD prendono spunto dal framework "SANS 20", pubblicato dal Center for Internet Security come "CCSC" (CIS Critical Security Controls for Effective Cyber Defense, nell'ottobre 2015), ampiamente diffuso a livello internazionale. Tale framework è composto da 20

controlli – Critical Security Controls (CSC) – ordinati sulla base dell'impatto sulla sicurezza dei sistemi; b) lavorando spesso per Pubbliche Amministrazioni, la Società in questo modo consente la verifica del livello di sicurezza garantito, ai sensi dell'art. 28, par. 3, lett. h del GDPR attraverso uno standard conosciuto dalla PA (in forza degli obblighi normativi direttamente applicabili), agevolando e semplificando le interlocuzioni con tali soggetti.

Analogamente, nei progetti che comportino la progettazione (preliminare/esecutiva) e lo sviluppo di sistemi informativi custom, nell'ottica dei principi di privacy & security by design e by default, adotta quale standard le Linee guida Agid per lo Sviluppo di Software sicuro per la Pubblica Amministrazione, rev. 1.0 del 21/11/2017.

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 della Qualità Certificato, l'Alta direzione effettua (anche ai sensi dell'art. 32, par. 1, lett. d del GDPR) effettua la verifica delle performance del framework per la data protection implementato; in particolare costituiscono oggetto di riesame:

- il registro dei trattamenti, al fine di verificare le necessità di aggiornamento dello stesso rispetto alle commesse acquisite nel periodo di riferimento
- gli esiti (in termini di copertura del fabbisogno formativo e di apprendimento) dell'attività formativa realizzata nel periodo sul tema
- il registro dei data breach (previsto dalla procedura precedentemente menzionata), in cui vengono censiti gli eventi (situazioni anomale o incidenti di sicurezza, considerati quali quasi-incidenti) nonché le vere e proprie violazioni di dati personali, a prescindere se l'evento abbia dato luogo alla notifica all'Autorità Garante e/o alla comunicazione agli interessati di cui agli artt. 33 e 34 GDPR e/o al Titolare del trattamento (nei casi in cui la violazione abbia coinvolto dati personali acquisiti nell'ambito di una o più commesse); il registro è strutturato in modo da consentire di identificare e circoscrivere (per "tipologia di eventi" ovvero per asset/trattamento) gli ambiti di criticità maggiormente impattanti - in termini organizzativi, operativi e di compliance - sull'organizzazione ed eventualmente sugli interessati, al fine di poter evidenziare i principali o più critici ambiti di intervento da gestire mediante azioni correttive
- il registro delle richieste di esercizio dei diritti degli interessati (previsto dalla procedura di cui al par. seguente); il registro è strutturato in modo da costituire non solo un fondamentale strumento documentale per tracciare e poter dimostrare la compliance sul punto, ma anche di individuare eventuali attività o modalità di trattamento considerate "critiche" dagli Interessati stessi

Il riesame è svolto congiuntamente dall'Alta direzione con il Responsabile Qualità ed il Privacy Manager 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.

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
- una attenta gestione dei loro diritti, secondo la specifica procedura adottata; il documento fornisce le istruzioni elative 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.

Segnalazioni di casi sospetti

Theorema incoraggia le segnalazioni di ogni problematica, criticità, violazione o non conformità relativa al trattamento di dati personali 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; alla casella di posta indicata accede esclusivamente la risorsa interna, autorizzata al trattamento, consistente nell'istruttoria della comunicazione pervenuta.

Al segnalante non anonimo è garantito un rigoroso regime di riservatezza sia in relazione alle proprie generalità, sia in ordine al contenuto della segnalazione che alla sua stessa effettuazione. L'eventuale violazione del predetto obbligo è fonte di responsabilità disciplinare interna.

Nei confronti del segnalante di sospetti in buona fede o di colui che segnala sulla base di convinzioni ragionevoli o confidenziali, non è consentita alcuna forma di ritorsione o discriminazione avente effetti sui rapporti contrattuali in essere ovvero sulla dignità della persona per motivi collegati alla denuncia stessa. Tuttavia, non sarà tollerata e sarà perseguita nelle forme legalmente possibili qualsiasi abuso della segnalazione quale, a titolo esemplificativo, la volontà di diffamare, calunniare o recare pregiudizio ingiustificato al segnalato od alla Società così come qualsiasi altra forma di strumentalizzazione per fini propri, di terzi e/o non corretti del presente istituto.

Roma, 17 febbraio 2023 Il Presidente