TITOLO: Politica per la sicurezza delle informazioni e protezione dei dati personali

SOMMARIO

TITOLO: Politica per la sicurezza delle informazioni e protezione dei dati personali

1. INTRODUZIONE

Scopo

Questa Politica è stata redatta per dimostrare l'impegno dell'Organizzazione a garantire la sicurezza delle informazioni di valore e a proteggere i dati personali.
L'obiettivo è garantire un trattamento delle informazioni trasparente, sicuro e conforme alle normative, nel rispetto dei requisiti cogenti applicabili, tra i quali la Norma ISO/IEC 27001 e lo standard VDA ISA 6.0.3 "Information Security Assessment Questionnaire", il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea e le Leggi italiane pertinenti.
Questa Politica si focalizza su un approccio che valorizza la fiducia degli interessati e tutela la reputazione dell'Organizzazione, assicurando al contempo un'operatività efficace ed efficiente.

Ambito di Applicazione

La presente Politica si applica a tutte le informazioni che hanno valore per TMB S.p.A., inclusi tutti i dati personali raccolti, trattati, memorizzati o trasferiti dall'Organizzazione, indipendentemente dal formato. Questo include, ma non si limita necessariamente a, informazioni relative a clienti, dipendenti, fornitori e altre parti interessate, nonché informazioni su prodotti realizzati da o per conto di questi Soggetti. La Politica riguarda tutte le unità organizzative, i collaboratori che in esse operano, nonché i terzi che trattano informazioni di valore, inclusi dati personali, per conto dell'Organizzazione.
Nei paragrafi che seguono, il termine "informazioni" verrà utilizzato per indicare una o più informazioni, di qualsiasi natura, che hanno valore per TMB S.p.A., inclusi quindi i dati personali. Analogamente, ove si richiamerà il tema della "sicurezza delle informazioni", si intenderà collettivamente la disciplina adottata da TMB S.p.A. per proteggere le informazioni di valore, inclusi i dati personali. Eventuali principi e disposizioni applicabili specificamente ai dati personali saranno opportunamente evidenziati nel testo.

Responsabilità e Governance

La responsabilità della gestione e del rispetto della presente Politica è attribuita al Comitato per la Sicurezza delle Informazioni, che include una rappresentanza dei vertici dell'Organizzazione e la figura del Referente Privacy, quest'ultimo coadiuvato da consulenti esterni. Tuttavia, la sicurezza delle informazioni è un dovere condiviso, e tutti i collaboratori che trattano informazioni aventi valore per TMB S.p.A. hanno la responsabilità di comprendere e aderire a questa Politica e a tutti i documenti che ne danno attuazione.

2. PRINCIPI FONDAMENTALI DELLA SICUREZZA DELLE INFORMAZIONI

Aspetti di sicurezza

L'Organizzazione riconosce che l'approccio alla sicurezza delle informazioni implica l'assunzione dell'impegno a preservare nel tempo:

- **Riservatezza**: la garanzia che l'informazione rimanga accessibile solamente alle entità autorizzate.
- **Integrità**: la garanzia che l'informazione mantenga nel tempo le sue caratteristiche di accuratezza e completezza rispetto al fatto, atto o entità che essa rappresenta.
- **Disponibilità**: la garanzia che l'informazione sia resa disponibile a una entità autorizzata che ne fa richiesta.

Fondamenti Legali e Normativi

L'Organizzazione si impegna a conoscere e rispettare i requisiti cogenti (Norme, Leggi e Regolamenti) applicabili alla sicurezza delle informazioni.
In particolare, questa Politica è in linea con i seguenti principi fondamentali:

1. **Necessità (*need to know*)**: i diritti di accesso a, ed effettuazione di trattamenti sulle informazioni di valore, sono concessi secondo un criterio di indispensabilità, negando per impostazione predefinita ogni diritto e privilegio che non sia strettamente indispensabile al corretto svolgimento dei trattamenti previsti.
2. **Fiducia nulla (*zero trust model*)**: ogni azione di trattamento su informazioni di valore viene per impostazione predefinita considerata potenzialmente dannosa e quindi governata come tale, indipendentemente dal fatto

che sia stata iniziata da un soggetto, un sistema informatico o un componente infrastrutturale operante sotto il controllo dell'Organizzazione.

Nell'ambito del trattamento dei dati personali, in conformità alle disposizioni del GDPR, valgono inoltre i principi che seguono:

1. **Liceità, correttezza e trasparenza**: i dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
2. **Limitazione della finalità**: i dati sono raccolti per scopi specifici, espliciti e legittimi, e non trattati ulteriormente in modo incompatibile con tali scopi.
3. **Minimizzazione dei dati**: i dati raccolti sono adeguati, pertinenti e limitati a ciò che è necessario rispetto agli scopi per i quali sono trattati.
4. **Esattezza**: i dati sono accurati e, se necessario, aggiornati; vengono adottate tutte le misure ragionevoli per garantire che i dati inesatti, rispetto agli scopi per i quali sono trattati, siano cancellati o rettificati senza indugio.
5. **Limitazione della conservazione**: i dati sono conservati in una forma che consente l'identificazione degli interessati per un periodo non superiore al conseguimento degli scopi per i quali i dati sono trattati.
6. **Integrità e riservatezza**: i dati sono trattati in modo da garantire una sicurezza adeguata dei dati personali, inclusa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danno accidentali, mediante l'adozione di misure tecniche o organizzative appropriate.

Conformità Pragmatica

L'Organizzazione adotta un approccio pragmatico alla conformità, con l'obiettivo di integrare i requisiti normativi in maniera che supportino gli obiettivi individuati. Ciò implica:

1. **Valutazione continua**: monitoraggio costante del quadro normativo pertinente al tema della sicurezza delle informazioni, per assicurare che le procedure e le prassi in essere siano sempre aggiornate e conformi.
2. **Integrazione tecnologica**: utilizzo di strumenti e tecnologie avanzate per semplificare la conformità; ad esempio, sistemi automatizzati per la gestione di diritti e privilegi di accesso, per l'ottenimento del consenso ai trattamenti, per il tracciamento e la gestione delle richieste degli interessati, per la tenuta dei registri e della documentazione in genere.

L'Organizzazione a tal scopo ha adottato un Modello Organizzativo per la Sicurezza delle Informazioni volto a delineare le modalità per governare il tema della sicurezza delle informazioni in conformità ai requisiti applicabili (normativa cogente e volontaria, in particolare il Regolamento GDPR, VDA ISA 6.0.3 "Information Security Assessment Questionnaire la Norma ISO/IEC 27001).

Minimizzazione dei Dati ed Efficienza

La raccolta e la preservazione di informazioni deve essere limitata a ciò che è strettamente necessario per i fini legittimi. Questo include:

1. Analisi della necessarietà delle informazioni: prima della raccolta delle informazioni, deve essere effettuata un'analisi per determinare la necessità e la pertinenza di tali informazioni rispetto agli scopi individuati.
2. Cancellazione delle informazioni: periodicamente, le informazioni non più necessarie per scopi legittimi vengono eliminate o anonimizzate.

Trasparenza e Comunicazione Chiara

L'Organizzazione si impegna a comunicare in modo chiaro e trasparente le pratiche relative al trattamento delle informazioni e alle misure tecniche e organizzative a presidio della sicurezza di tali informazioni. Ciò comprende:

1. Policy e procedure documentate: le misure tecniche e organizzative per la sicurezza delle informazioni devono, come necessario, essere accompagnate da una descrizione documentata delle rispettive modalità di attuazione.

2. Informative: devono essere fornite informative sulla privacy che siano facilmente accessibili e comprensibili, anche in forma schematica, spiegando come e perché i dati personali sono raccolti e utilizzati.
2. Comunicazione proattiva: gli interessati devono essere informati in caso di modifiche significative nelle pratiche di trattamento dei dati o nelle politiche di privacy.

3. DIRITTI DEGLI INTERESSATI

L'Organizzazione riconosce e rispetta tutti i diritti degli interessati in conformità con il GDPR e le leggi italiane. Si adottano procedure semplificate per:

1. Accesso ai Dati: consentire agli interessati di accedere facilmente ai propri dati personali.
2. Rettifica e cancellazione: fornire meccanismi semplici per la rettifica o la cancellazione dei dati personali.
3. Opposizione al trattamento: consentire agli interessati di opporsi al trattamento dei loro dati quando ricorrano determinate circostanze.

4. GESTIONE DELLE INFORMAZIONI E PROCESSI DELL'ORGANIZZAZIONE

L'integrazione efficace della sicurezza delle informazioni nei processi dell'Organizzazione è fondamentale. Ciò include:

1. Valutazione del rischio: condurre valutazione del rischio regolari per identificare e mitigare i potenziali rischi associati al trattamento di informazioni di valore.
2. Procedure flessibili: sviluppare politiche che permettano adeguamenti in base alle mutevoli esigenze dell'Organizzazione e normative.
3. Miglioramento continuo: trarre il massimo insegnamento dalle circostanze che si sperimentano sia nella normale operatività quotidiana, sia a maggior ragione in occasione di situazioni anomale o critiche per la sicurezza delle informazioni (come ad esempio nel caso di incidenti di sicurezza) e sfruttare le lezioni apprese per migliorare costantemente il modello organizzativo per la sicurezza delle informazioni e la privacy.

5. SICUREZZA DELLE INFORMAZIONI

Misure di Sicurezza

Per proteggere le informazioni da violazioni di riservatezza (accessi o divulgazioni non autorizzati), integrità (alterazioni non autorizzate) e disponibilità (cancellazioni o altre circostanze accidentali o deliberate che comportino l'impossibilità di accedere a una informazione), l'Organizzazione implementa misure di sicurezza adeguate, che includono:

1. Protezioni tecniche: adozione di soluzioni fisiche e tecnologiche come la chiusura degli armadi, la crittografia, il controllo degli accessi e la sicurezza delle reti, che siano efficaci ma non intralcino le operazioni quotidiane, in quanto questo tipicamente incide sulla reale applicabilità delle stesse.
2. Procedure organizzative: definizione di procedure chiare per la gestione dei dati, compresi i protocolli per la condivisione di informazioni all'interno dell'Organizzazione e per il trasferimento sicuro da e verso Soggetti esterni.

Gestione Proattiva degli incidenti di sicurezza

In caso di incidenti di sicurezza, inclusa la violazione dei dati personali, l'Organizzazione segue una procedura ben definita:

1. Rilevamento e risposta rapida: identificazione e risposta tempestiva alle violazioni per minimizzare l'impatto.
2. Notifica di violazione: comunicazione delle violazioni alle autorità di controllo e agli interessati, come richiesto dalla Legge.
3. Revisione e prevenzione: analisi delle cause delle violazioni e implementazione di misure per prevenire incidenti futuri.

Trasferimenti Internazionali di dati personali

Il trasferimento internazionale di dati personali è gestito con attenzione per garantire la conformità con il GDPR e altre leggi pertinenti contemperando la preferenza per fornitori e tecnologie UE alla scelta di tecnologie e soluzioni eventualmente disponibili extra-UE. In ogni caso verranno valutate preferenzialmente:

1. Clausole contrattuali: utilizzo di clausole contrattuali standard e altre misure legali per garantire la protezione dei dati quando vengono trasferiti al di fuori dell'Unione Europea.
2. Valutazioni di adeguatezza: valutazione delle leggi sulla protezione dei dati nei paesi destinatari per assicurare un livello adeguato di protezione.

Formazione e Consapevolezza

Per garantire che tutti i collaboratori comprendano l'importanza del contributo di ciascuno alla sicurezza delle informazioni e sappiano come trattare in modo sicuro le informazioni, l'Organizzazione offre:

1. Programmi di formazione regolari: formazione continua su temi quali la sicurezza delle informazioni in generale, la cybersecurity, la conformità alle disposizioni del GDPR e le migliori pratiche di sicurezza.
2. Materiale formativo: disponibilità di risorse formative, come manuali e guide online, per supportare la comprensione e l'attuazione delle politiche di sicurezza delle informazioni.

Monitoraggio, Valutazione e Aggiornamento

Per assicurare che le politiche e le pratiche rimangano efficaci e pertinenti, l'Organizzazione si impegna a:

1. Audit e valutazioni: condurre audit interni e valutazioni del rischio per monitorare la conformità e l'efficacia delle misure tecniche e organizzative per la sicurezza delle informazioni.
2. Aggiornamenti continui: aggiornare le politiche e le procedure in risposta ai cambiamenti normativi, tecnologici o di business, per garantire che la sicurezza delle informazioni rimanga effettiva.

Aspetti disciplinari

L'orientamento alla sicurezza delle informazioni e alla protezione dei dati personali non è solamente la conseguenza di un obbligo dettato da Norme, Leggi e Regolamenti vigenti o da impegni assunti contrattualmente con i Clienti, ma è anche e soprattutto una scelta consapevole di TMB al fine di favorire, e conservare nel tempo, la fiducia di tutte le parti interessate (Clienti, Istituzioni, Autorità) con cui l'Azienda interagisce.
Una fattiva collaborazione da parte di tutti i soggetti coinvolti, siano essi interni ed esterni a TMB, nel conoscere e rispettare policy, procedure e norme interne emanate da TMB per la sicurezza delle informazioni e la protezione dei dati personali, è un fattore imprescindibile per garantire che il livello di sicurezza effettivamente raggiunto sul campo corrisponda agli impegni assunti e agli obiettivi posti dall'Azienda in tale ambito.
Il Personale aziendale è tenuto pertanto a conoscere e applicare correttamente le disposizioni stabilite da TMB in materia di sicurezza delle informazioni e protezione della privacy. Episodi di violazione di informazione di valore o di dati personali che, a seguito di analisi interne, siano riconducibili a comportamenti inappropriati (mancato rispetto di policy e procedure per imprudenza, noncuranza o atto deliberato) potranno comportare a carico del responsabile l'irrogazione di provvedimenti disciplinari, nel rispetto della Legislazione pertinente.

Ultimo aggiornamento: 27/01/2025