Nome del documento / procedura	Sezione:	Livello di riservatezza:
POLITICA PER LA PROTEZIONE DEI DATI	**ACCOUNTABILITY**	**Pubblico**

Politica per la protezione dei dati in recepimento del Reg. UE 2016/679 - Legge 21/12/2018 n. 171 della Repubblica di San Marino al fine di garantire e tutelare i diritti e le libertà fondamentali delle persone fisiche

INDICE

1. SCOPO

Scopo del presente documento è quello di descrivere la politica dell'organizzazione, le modalità e le procedure generali per il trattamento nonché per la sicurezza e riservatezza dei dati e delle informazioni.
Tale politica è applicata sia per i trattamenti dati svolti in qualità di "Titolare del trattamento" che in qualità di "Responsabile del trattamento" e garantisce ed assicura a tutti i soggetti interessati coinvolti nell'ambito del trattamento dei dati una adeguata protezione attraverso l'adozione di un "Sistema di gestione dei dati personali" nel rispetto dei diritti e le libertà fondamentali delle persone, in ottemperanza al Regolamento Europeo 2016/679, d'ora in avanti GDPR e dalla Legge 21/12/2018 n. 171 della Repubblica di San Marino.

2. DESCRIZIONE

Obiettivi perseguiti

La nostra organizzazione intende perseguire obiettivi di sicurezza delle informazioni, dei dati personali, della struttura tecnologica, fisica, logica ed organizzativa e della loro gestione. Questo significa raggiungere e mantenere un sistema di gestione sicura delle informazioni attraverso il rispetto dei principi previsti dagli articoli 5 e 6 del GDPR e degli articoli 4 e 5 della Legge 21/12/2018 n. 171 della Repubblica di San Marino;

- ✓ Liceità, correttezza, trasparenza;
- ✓ Garanzia rispetto alla gestione e raccolta dei dati per le sole finalità contrattuali, determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. Tali garanzie sono applicate e verificate anche a cascata nei confronti degli eventuali subfornitori (subresponsabili);
- ✓ Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati");
- ✓ Esatti e, se necessario, aggiornati devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
- ✓ Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- ✓ Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali "principio di integrità e riservatezza";
- ✓ Assicurare che i dati personali siano accessibili solamente ai soggetti e/o alle categorie degli stessi debitamente autorizzati;
- ✓ Salvaguardare la consistenza dell'informazione da modifiche non autorizzate;

- ✓ Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati in riferimento ai ruoli e mansioni ricoperti;
- ✓ Assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
- ✓ Garantire l'affidabilità dei canali di provenienza delle informazioni;
- ✓ Garantire la protezione ed il controllo dei dati personali.

Istruzioni, compiti e funzioni, formazione

Considerato che il GDPR all'art. 29 e il D.Lgs. 196/2003 all'art. 2 quaterdecies e l'articolo 30 della Legge 21/12/2018 n. 171 della Repubblica di San Marino prevede che tutti i soggetti designati autorizzati al trattamento dei dati, con compiti e funzioni definiti, sotto l'autorità del titolare o del responsabile debbano essere debitamente istruiti e quindi formati sui compiti, responsabilità e per l'effettuazione delle operazioni di trattamento dei dati, nonché si impegnino alla riservatezza, l'Organizzazione ha redatto un piano di formazione sulla base dei ruoli e mansioni interne in funzione degli specifici trattamenti dati e dei rischi valutati.

La formazione è pensata e realizzata per le mansioni ed i ruoli ricoperti dal personale dipendente e dai collaboratori ed ha le seguenti caratteristiche:

a) Specifica - corrispondente alla tipologia di mansione/ruolo svolto;
b) Appropriata - in relazione alla tipologia dei trattamenti dati realizzati;
c) Permanente - deve prevedere una programmazione temporale ed un aggiornamento periodico in particolare per eventuali nuovi assunti;
d) Documentata - il suo svolgimento ed i successivi aggiornamenti devono risultare da registri, attestati o altre forme che ne diano evidenza;
e) Efficace – deve essere verificata periodicamente la comprensione generale, specifica ed il recepimento delle procedure adottate

Nei confronti dei nostri fornitori che si qualificano quali responsabili del trattamento:
Tali principi e garanzie sono verificate per ogni nostro fornitore il cui servizio prevede il trattamento di dati personali, attraverso la stipula di clausole o contratti che prevedono istruzioni per il trattamento dei dati ai sensi dell'art 28 del GDPR. Viene inoltre monitorato sistematicamente lo stato di implementazione di tali garanzie.

3. AMBITO DI APPLICAZIONE

La politica per la protezione dei dati personali si applica a tutto il personale interno e si condivide con le terze parti che collaborano alla condivisione e gestione delle informazioni nonché a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.
Tale politica viene applicata per le attività principali ed accessorie del titolare del trattamento dei dati che sono descritte nel registro delle attività del trattamento.

4. ADEMPIMENTI E PROCEDURE ADOTTATE DALL'ORGANIZZAZIONE

Adempimenti e procedure adottate dall'organizzazione, previste dal Regolamento UE 2016/679 e dalla Legge 21/12/2018 n. 171 della Repubblica di San Marino e per le quali si richiede la compliance ai nostri partner

- La verifica dei dati che saranno oggetto di trattamento con identificazione delle varie tipologie di dati e delle categorie di appartenenza. La verifica della finalità di ogni trattamento e della base giuridica sul quale ciascuno di essi si fonda.

- La predisposizione della/delle informazioni sul trattamento dei dati (o il loro aggiornamento) che devono essere fornite agli interessati nel rispetto di tutti gli elementi indicati agli artt. 13 e 14 del GDPR e della Legge 21/12/2018 n. 171 della Repubblica di San Marino. In particolare gli interessati dovranno essere messi a conoscenza dei diritti che il GDPR riconosce loro (diritto di accesso, diritto di cancellazione, diritto di rettifica, diritto di limitazione e di opposizione al trattamento, diritto alla portabilità dei dati);

- L'organizzazione adotta procedure di "Privacy by design e by default" in riferimento all'art. 25 del GDPR, al fine di verificare sia al momento della determinazione dei mezzi, sia all'atto del trattamento stesso / introduzione di nuovi strumenti che prevedono trattamenti dati, le misure tecniche organizzative adeguate sulla base della valutazione del rischio. Secondo il disposto del paragrafo 2 art. 25, l'organizzazione mette in atto misure tecniche e organizzative adeguate (quali in primis le istruzioni / formazione agli addetti) per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, e non siano resi accessibili dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica.

- L'individuazione dei soggetti in qualità di "Responsabili del trattamento" in riferimento all'art. 28 del GDPR che svolgono dei compiti per conto del titolare del trattamento, nonché la stipula di accordi / contratti adeguati al livello di rischio derivante dai trattamenti dati affidati.

- La predisposizione del registro delle attività di trattamento dei dati personali sia in qualità di titolare, che in qualità di responsabile (ove applicabile), qualora esso risulti necessario in base al disposto dell'art. 30 del GDPR e dall'art. 31 della Legge 21/12/2018 n. 171 della Repubblica di San Marino, ossia nel caso in cui l'organizzazione che effettua il trattamento dei dati abbia più di 250 dipendenti. Tale registro dovrà essere redatto anche nel caso in cui l'impresa od organizzazione abbia meno di 250 dipendenti, ma ponga in essere un trattamento dei dati che presenta un potenziale rischio per i diritti e libertà degli interessati il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

- L'instaurazione di una procedura da adottare in caso di eventuali violazioni dei dati (c.d. Data Breach di cui agli articoli 33 e 34 del GDPR e 34 e 35 della Legge 21/12/2018 n. 171 della Repubblica di San Marino), ad esempio al verificarsi di una divulgazione (intenzionale o meno), della distruzione, della perdita, della modifica o dell'accesso non autorizzato ai dati personali oggetto di trattamento. Il GDPR e la Legge 21/12/2018 n. 171 della Repubblica di San Marino prevedono infatti degli specifici adempimenti nel caso in cui si verifichi una violazione di tal genere, a causa di un attacco informatico, di un accesso abusivo o di un incidente. In questi casi il GDPR impone, in capo al Titolare del trattamento l'obbligo di comunicare all'autorità di controllo l'avvenuta violazione entro 72 ore (o comunque senza ritardo). Nel caso in cui la violazione verificatasi faccia presumere che vi sia anche un elevato e attuale pericolo per i diritti e le libertà degli interessati, anche questi ultimi dovranno essere direttamente informati senza ritardo di quanto successo. A Tale riguardo è necessario che l'organizzazione sia dotata di un registro degli incidenti.

- All'art. 35 del GDPR e all'art. 36 della Legge 21/12/2018 n. 171 della Repubblica di San Marino, si configura, in capo al Titolare del trattamento (e con la possibilità di consultare il Responsabile della protezione dei dati se nominato), l'obbligo di procedere ad una valutazione d'impatto sulla protezione dei dati nel caso in cui un tipo di trattamento, anche in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso, presenti un rischio elevato per i diritti e le libertà delle persone fisiche.

- Agli articoli 37 – 38 e 39 del GDPR e 38 – 39 e 40 della Legge 21/12/2018 n. 171 della Repubblica di San Marino viene introdotto un altro adempimento richiesto al Titolare del trattamento che consiste nella designazione del Responsabile della protezione dei dati RPD, definito altresì DPO - Data Protection Officer. Tale nomina, come previsto dall'art. 37 del GDPR, è obbligatoria soltanto in una serie di ipotesi, in particolare, nel caso in cui il trattamento dei dati sia effettuato da un'autorità pubblica o da un organismo pubblico; quando le attività principali svolte del titolare o del responsabile del trattamento consistono in operazioni che, per la loro natura, l'ambito di applicazione o le finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala; e infine nel caso in cui le attività principali effettuate consistano nel trattamento, su larga scala, di dati sensibili o di dati relativi a condanne penali e a reati consistenti nell'illecito trattamento dei dati personali. Come suggerito anche dall'ex-WP29, oggi EDPB, l'organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro che ha predisposto le Linee guida dettando regolare sulla nomina del Responsabile per la protezione dei dati personali; quando il Regolamento non impone specificamente la nomina di un DPO, questa figura potrà comunque essere designata dal titolare o dal responsabile del trattamento su base volontaria.

Istruzioni per i soggetti interni e/o esterni che si interfacciano con l'organizzazione

Particolare importanza viene attribuita alle procedure del Sistema di Gestione per la Protezione dei dati personali, indicate nelle istruzioni e formazione che sono fornite al personale ed alle quali vi è l'obbligo di attenersi scrupolosamente. Le istruzioni fornite agli addetti designati ai trattamenti dati costituiscono politica aziendale per il trattamento dei dati, e vengono revisionate e/o aggiornate almeno una volta all'anno.

5. RESPONSABILITÀ PER L'ADOZIONE DELLA POLITICA

L'organizzazione sia in qualità di "Titolare del trattamento" che in qualità di "Responsabile del trattamento" è responsabile della politica per la protezione dei dati, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- Evoluzioni significative del business;
- Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- Significativi incidenti di sicurezza;
- Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;

6. RIESAME AD AGGIORNAMENTO DELLA POLITICA

Periodicamente, almeno una volta all'anno, dovrà essere svolto un riesame per la verifica dell'efficienza e dell'efficacia, nonché dell'adeguatezza delle misure tecniche/organizzative applicate, nel rispetto ed al fine ultimo della protezione dei dati, diritti e libertà fondamentali delle persone.

Per approvazione

_____

(Data, Timbro e Firma)