POLITICA SULLA PROTEZIONE DEI DATI PERSONALI (PRIVACY POLICY)

Campo d'applicazione, scopo e destinatari

L'Associazione La Pietra Verde, in seguito denominata "Associazione", si impegna a rispettare le leggi ed i regolamenti applicabili relativi alla protezione dei dati personali nei paesi in cui l'Ente opera.

Questa Politica stabilisce i principi di base con cui l'Associazione tratta i dati personali dei consumatori ed altri utenti in genere di cui ne tratta dati personali ed indica le responsabilità dei propri dipartimenti interni e dei propri dipendenti durante il trattamento dei dati personali.

La presente politica si applica e si rende necessaria per le attività svolte all'interno dello Spazio Economico Europeo (SEE) o per i dati personali degli interessati all'interno del SEE.

I destinatari di questo documento sono tutti i consumatori e gli utenti che usufruiscono dei servizi dell'Ente.

Documenti di Riferimento

- Il GDPR dell'UE 2016/679 (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)
- Il D.Lgs.196/2003 c.d. "TESTO UNICO DELLA PRIVACY"
- Politica di Conservazione dei Dati
- Descrizione dei Ruolo del Responsabile della Protezione dei Dati
- Linee guida per l'Elenco dei Dati e la Mappatura delle Attività di Trattamento
- Procedura per la Richiesta di Accesso ai Dati da parte dell'Interessato
- Procedura di Comunicazione di una Violazione di Dati

Definizioni

Le seguenti definizioni di termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (o GDPR):

Dato Personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati personali sensibili: Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, le

opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Controllore dei Dati (TITOLARE DEL TRATTAMENTO): La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Processore dei Dati (RESPONSABILE DEL TRATTAMENTO): una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Controllore.

Addetto al Trattamento: persona fisica la cui mansione è quella di raccogliere e trattare con o senza l'ausilio di processi automatizzati dati personali o insiemi di dati personali**.**

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Anonimizzazione: Deidentificazione irreversibile dei dati personali in modo tale che la persona non possa essere identificata utilizzando tempi, costi e tecnologie ragionevoli da parte del controllore o di qualsiasi altra persona per identificare l'interessato. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile.

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. La pseudonimizzazione riduce, ma non elimina completamente, la possibilità di collegare il dato personale all'interessato. Poiché i dati pseudominizzati sono comunque dati personali, il trattamento dei dati pseudonimizzati dovrebbe essere conforme ai principi del Trattamento dei Dati Personali.

Trattamento transfrontaliero: il trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un controllore o processore dei dati nell'Unione ove il controllore o il processore siano stabiliti in più di uno Stato membro; oppure il trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un controllore o processore nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE;

Autorità di Controllo Capofila: L'autorità di controllo con la responsabilità primaria di gestire un'attività di trattamento di dati transfrontaliera, ad esempio quando un interessato presenta un reclamo in merito al trattamento dei propri dati personali; è responsabile, tra l'altro, di ricevere le notifiche di violazione dei dati, di essere notificato su attività di trattamento rischiose e avrà piena autorità per quanto riguarda le sue funzioni per garantire l'osservanza delle disposizioni del GDPR dell'UE;

Ogni "**autorità di controllo locale**" manterrà comunque nel proprio territorio e monitorerà qualsiasi trattamento di dati locale che incide sugli interessati o che viene effettuato da un controllore o un processore all'interno dell'Unione oppure all'esterno dell'Unione in caso il loro trattamento si rivolge a interessati residenti sul proprio territorio. I loro compiti e poteri comprendono lo svolgimento di indagini e l'applicazione di misure amministrative e sanzioni, la promozione della consapevolezza da parte del pubblico dei rischi, delle norme, della sicurezza e dei diritti in relazione al trattamento dei dati personali, nonché l'accesso a qualsiasi sede del controllore e del processore dei dati, compresi eventuali strumenti e mezzi per il trattamento.

"Stabilimento principale per quanto riguarda un controllore" con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del controllore nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

"Stabilimento principale con riferimento a un processore" responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

"Gruppo imprenditoriale": un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

Principi Applicabili al Trattamento dei Dati Personali

I principi applicabili alla protezione dei dati delineano le responsabilità delle organizzazioni nella gestione dei dati personali. L'articolo 5 (2) del GDPR enuncia che "*il controllore è competente per il rispetto dei principi, e in grado di comprovarlo*."

Liceità, Correttezza e Trasparenza

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

Limitazione delle Finalità

I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

Minimizzazione dei Dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati. L'Ente deve applicare l'anonimizzazione o la pseudonimizzazione ai dati personali, se possibile, per ridurre il rischio per gli interessati.

Esattezza

I dati personali devono essere 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.

Limitazione del Periodo di Conservazione

I dati personali devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Integrità e riservatezza

Tenendo conto delle tecnologie e di altre misure di sicurezza disponibili, dei costi di attuazione e la probabilità e gravità dei rischi per i dati personali, l'Ente deve mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato per i dati personali, inclusa la protezione dalla distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.

Responsabilizzazione

I controllori dei dati sono competenti per il rispetto dei principi sopra descritti devono essere in grado di comprovarlo.

Costruire la protezione dei dati nelle attività commerciali

Al fine di dimostrare la conformità con i principi della protezione dei dati, un'organizzazione dovrebbe creare alti profili di protezione dei dati nelle sue attività.

Notifica agli Interessati

(Vedi Linee guida sul Corretto Trattamento.)

Scelta e Consenso dell'Interessato

(Vedi Linee guida sul Corretto Trattamento.)

Raccolta

L'Ente deve sforzarsi di raccogliere il minor numero di dati personali possibili.

Se i dati personali sono raccolti da terzi, i responsabili dei trattamenti dei vari comparti, devono garantire che i dati personali siano raccolti legalmente.

Uso, Conservazione e Smaltimento

Le finalità, i metodi, il limite di registrazione e il periodo di conservazione dei dati personali devono essere coerenti con le informazioni contenute nell'Informativa sulla Privacy. L'Ente deve mantenere l'esattezza, l'integrità, la riservatezza e la rilevanza dei dati personali in base allo scopo del trattamento.

È necessario utilizzare adeguati meccanismi di sicurezza volti a proteggere i dati personali per impedire che vengano rubati, utilizzati in modo improprio o abusati e prevenire le violazioni dei dati personali.

Il Responsabile della Protezione dei Dati è responsabile della conformità con i requisiti elencati in questa sezione.

Divulgazione a terzi

Ogni volta che l'Ente utilizza un fornitore o un partner terzo per il trattamento dei dati personali per suo conto, il Responsabile della Protezione dei Dati deve garantire che questo processore fornisca misure di sicurezza per salvaguardare i dati personali adeguate ai rischi associati.

A tal fine, è necessario utilizzare il Questionario di Conformità del Processore al GDPR.

L'Ente deve richiedere contrattualmente al fornitore di fornire lo stesso livello di protezione dei dati e comunque sempre il più elevato standard di sicurezza dei dati al momento del trattamento.

Il fornitore o il partner devono trattare i dati personali solo per adempiere ai propri obblighi contrattuali nei confronti dell'Ente o dietro istruzioni dell'Ente e non per altri scopi.

Quando l'Ente tratta i dati personali congiuntamente con un terzo indipendente, l'Ente deve specificare esplicitamente le responsabilità proprie e quelle del terzo nel relativo contratto o in qualsiasi altro documento legale vincolante, quale l'Accordo con il Fornitore del Trattamento dei Dati.

Trasferimento Transfrontaliero dei Dati Personali

Prima di trasferire i dati personali dallo Spazio Economico Europeo (SEE) devono essere utilizzate misure di protezione adeguate, compresa la firma di un accordo sul trasferimento dei dati, come richiesto dall'Unione Europea e, se necessario, deve essere ottenuta l'autorizzazione della relativa Autorità per la Protezione dei Dati. L'entità che riceve i dati personali deve rispettare i principi del trattamento dei dati personali stabiliti nella Procedura di Trasferimento Transfrontaliero di Dati Personali.

Diritto d'Accesso da parte degli Interessati

Il TITOLARE DEL TRATTAMENTO è responsabile di fornire agli interessati un adeguato meccanismo di accesso ai propri dati personali.

L'accesso dovrà consentire all'interessato di aggiornare, rettificare, cancellare e/o trasmettere i propri dati personali.

Il meccanismo di accesso sarà ulteriormente dettagliato nella Procedura di Richiesta di Accesso ai Dati da parte dell'Interessato.

Portabilità dei Dati

Gli interessati hanno il diritto di ricevere, su esplicita richiesta, una copia dei dati che hanno fornito.

I dati dovranno essere forniti in un formato strutturato e potranno (previa esplicita richiesta) essere trasmessi a un altro controllore, gratuitamente e sempre esclusivamente su richiesta dell'interessato.

Il Responsabile della Protezione dei Dati è responsabile di garantire che tali richieste vengano elaborate entro un mese e non incidano sui diritti relativi ai dati personali di altre persone.

Diritto all'oblio

Su richiesta, gli interessati hanno il diritto di ottenere dall'Ente la cancellazione dei propri dati personali (diritto all'oblio).

Quando l'Ente agisce come Controllore, il RESPONSABILE DEL TRATTAMENTO DI COMPARTO deve intraprendere le azioni necessarie (comprese le misure tecniche) per informare i terzi che utilizzano o trattano tali dati per conformarsi alla richiesta.

Linee guida sul Corretto Trattamento

I dati personali devono essere trattati solo se esplicitamente autorizzati dall'INTERESSATO.

L'Ente deve decidere se eseguire la Valutazione d'Impatto sulla Protezione dei Dati per ciascuna attività di trattamento dei dati in base alle Linee guida sulla Valutazione d'Impatto sulla Protezione dei Dati.

Comunicazioni agli Interessati

Al momento della raccolta o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento, inclusa l'erogazione dei servizi, Il Controllore (TITOLARE DEL TRATTAMENTO) è responsabile di informare adeguatamente gli interessati di quanto segue: i tipi di dati personali raccolti, le finalità del trattamento, I metodi di trattamento, i diritti degli interessati riguardo ai loro dati personali, il periodo di conservazione, i potenziali trasferimenti internazionali di dati, se i dati saranno condivisi con terzi e le misure di sicurezza dell'Ente per proteggere i dati personali.

Queste informazioni saranno fornite tramite un'Informativa sulla Privacy.

Laddove i dati personali siano condivisi con terzi, il Responsabile della Protezione dei Dati deve garantire che gli interessati siano stati informati di ciò tramite un'Informativa sulla Privacy.

Laddove i dati personali siano trasferiti in un paese terzo in base alla politica di trasferimento transfrontaliero dei dati, l'Informativa sulla Privacy dovrà riportarlo e indicare chiaramente dove e a quale soggetti i dati personali vengono trasferiti.

Nel caso in cui vengano raccolti dati personali sensibili, il Responsabile della Protezione dei Dati deve assicurarsi che l'Informativa sulla Privacy riporti esplicitamente lo scopo per il quale tali dati personali sensibili vengono raccolti.

Ottenere i Consensi

Ogni volta che il trattamento dei dati personali si basa sul consenso dell'interessato, o su altri motivi legittimi, il Processore (Il responsabile del trattamento) di ogni comparto dell'Ente è responsabile della conservazione di una registrazione di tale consenso.

Il Titolare del Trattamento (Controllore) è responsabile di fornire agli interessati le opzioni per dare il consenso e deve informarli e garantire che il loro consenso (ogni volta che il consenso venga utilizzato come base legale per il trattamento) possa essere revocato in qualsiasi momento.

Laddove la raccolta di dati personali si riferisca a un minore di età inferiore ai 16 anni, il Responsabile della Protezione dei Dati deve garantire che il consenso del titolare della responsabilità genitoriale sia fornito prima della raccolta utilizzando il modulo di consenso del titolare della responsabilità genitoriale.

Quando si richiede di correggere, modificare o distruggere le registrazioni dei dati personali, il Responsabile della Protezione dei Dati deve garantire che tali richieste siano gestite entro un ragionevole lasso di tempo. Il Responsabile della Protezione dei Dati deve anche registrare le richieste e tenere un registro di queste.

I dati personali devono essere trattati solo per le finalità per cui sono stati originariamente raccolti. Nel caso in cui l'Ente desideri trattare i dati personali raccolti per un altro scopo, l'Ente deve richiedere il consenso degli interessati in forma scritta chiara e concisa. Qualsiasi richiesta di questo tipo dovrebbe includere lo scopo originale per cui sono stati raccolti i dati e anche gli scopi nuovi o aggiuntivi. La richiesta deve includere

anche il motivo del cambiamento di scopo / i. Il Responsabile della Protezione dei Dati è responsabile del rispetto delle regole in questo paragrafo.

Il Responsabile della Protezione dei Dati deve garantire che i metodi di raccolta siano conformi alla legge, alle buone pratiche e alle norme regolamentari.

Il Responsabile della Protezione dei Dati è responsabile della creazione e della manutenzione di un registro delle Informative sulla Privacy.

Organizzazione e Responsabilità

La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque lavori per o con l'Associazione e abbia accesso ai dati personali trattati dall'Associazione.

Le principali aree di responsabilità per il trattamento dei dati personali sono i seguenti ruoli organizzativi:

Il Consiglio Direttivo prende decisioni e approva le strategie generali dell'Ente in materia di protezione dei dati personali.

Il **Responsabile della Protezione dei Dati,** è responsabile della gestione del programma di protezione dei dati personali ed è responsabile dello sviluppo e della promozione delle politiche di protezione dei dati personali dall'inizio alla fine, come definito nella Descrizione del Ruolo del Responsabile della Protezione dei Dati; monitora e analizza le leggi sui dati personali e le modifiche alle normative, sviluppa i requisiti di conformità e assiste nel raggiungimento degli obiettivi relativi ai dati personali. È inoltre responsabile di:

- Garantire che tutti i sistemi, i servizi e le attrezzature utilizzati per la registrazione dei dati soddisfino standard di sicurezza accettabili.
- Condurre controlli e scansioni regolari per garantire che l'hardware e il software di sicurezza funzionino correttamente.
- Migliorare la consapevolezza di tutti i dipendenti sulla protezione dei dati personali degli utenti.
- Organizzare la formazione per la competenza e la sensibilizzazione sulla protezione dei dati personali per i dipendenti che lavorano con dati personali.
- Garantire che i dati personali dei dipendenti vengano trattati in base alle legittime finalità e necessità dell'Associazione.
- Trasferire le responsabilità di protezione dei dati personali ai fornitori e del miglioramento dei livelli di consapevolezza dei fornitori in materia di protezione dei dati personali, nonché del flusso verso il basso dei dati personali richiesti a qualsiasi fornitore terzo che l'Associazione utilizzi.

Risposta agli incidenti di Violazione dei Dati Personali

Quando l'Associazione viene a conoscenza di una presunta o effettiva violazione dei dati personali, deve eseguire un'indagine interna e adottare misure correttive appropriate in modo tempestivo, in base alla Politica sulla violazione dei dati. Laddove sussistano rischi per i diritti e le libertà degli interessati, l'Associazione deve informare l'autorità di controllo competente in materia di protezione dei dati senza indebiti ritardi e, ove possibile, entro 72 ore.

Audit e Responsabilizzazione

Il Responsabile della Protezione dei Dati è responsabile di verificare in che modo l'Associazione implementi questa politica.

Qualsiasi dipendente che violi questa Politica sarà soggetto ad azioni disciplinari e potrebbe anche essere soggetto a responsabilità civili o penali qualora la sua condotta violasse leggi o regolamenti.

Conflitti con la Legge

Questa politica è intesa a rispettare le leggi italiane ed i regolamenti europei.

In caso di conflitto tra questa Politica e le leggi e i regolamenti applicabili, prevarranno questi ultimi.

Gestione delle registrazioni sulla base di questo documento

Nome del documento	**Persona responsabile dell'archiviazione**	**Controlli per la protezione del documento**	**Tempo di archiviazione**
Modulo di Consenso dell'Interessato	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso ai moduli	5 anni
Modulo di Recesso dell'Interessato	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso ai moduli	5 anni
Modulo di Consenso dei Titolari della Responsabilità Genitoriale	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso ai moduli	5 anni
Modulo di Recesso dei Titolari della Responsabilità Genitoriale	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso ai moduli	5 anni
Registro delle Informative sulla Privacy	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso alla cartella	Permanente

Validità e gestione del documento

Questo documento ha effetto dal 25/05/2018.

Il responsabile per questo documento è il Responsabile della Protezione dei Dati, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.