02.1 - POLITICA SULLA PROTEZIONE DEI DATI PERSONALI

Marco Zelinotti

Dottore Commercialista

Sede Legale: Via G. Garibaldi, 27 - 00047 Marino (RM)

Tel. 06.97608221 - Fax 06.9385797

e-mail: marco.zelinotti@studiozelinotti.it

Sommario

02.1 - POLITICA SULLA PROTEZIONE DEI DATI PERSONALI

1. Campo d'applicazione, scopo e destinatari

Compito del detentore dei dati è quello di rispettare le leggi e i regolamenti che disciplinano la protezione dei dati personali.

Questa Politica stabilisce i principi posti alla base del trattamento dei dati personali dei consumatori ed altri utenti in genere.

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 fruitori dei servizi offerti da **Studio ZELINOTTI**

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 Protezione dei Dati Personali dei Dipendenti
- Politica di Conservazione dei Dati
- Descrizione del 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
- Metodologia di Valutazione d'Impatto sulla Protezione dei Dati
- Procedura di Trasferimento Transfrontaliero di Dati Personali
- Politiche di Sicurezza IT
- Procedura di Comunicazione di Violazione di Dati

2. Definizioni

I termini utilizzati in questo documento sono estrapolati 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.

Titolare del trattamento dati: 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.

Responsabile del trattamento dati: una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento dati.

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 applicati 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 Titolare del trattamento dati 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 fatto 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 e degli stabilimenti che un Titolare o Responsabile del trattamento ha in più di uno Stato membro dell'Unione; oppure il trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile del trattamento dati stabilito nell'Unione, ma che incide in modo più o meno sostanziale su più 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 e destinataria di eventuali reclami attinenti al trattamento dei dati personali; è responsabile, tra l'altro, di ricevere le comunicazioni attinenti alla violazione dei dati e all'attività di trattamento rischiose e avrà piena autorità funzionale per garantire l'osservanza delle disposizioni del GDPR dell'UE;

Ogni "**autorità di controllo locale**" nel proprio territorio monitorerà qualsiasi trattamento di dati locali in grado di incidere sugli interessati o che viene effettuato da un Titolare del trattamento dati o un Responsabile del trattamento dati all'interno dell'Unione o all'esterno dell'Unione. Rientra nei suoi compiti 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 ai dati in qualsiasi sede da parte del Titolare del trattamento dati e del Responsabile del trattamento dati, compresi eventuali strumenti e mezzi per il trattamento.

"Stabilimento principale del Titolare del trattamento dati": qualora il Titolare del trattamento dati abbia stabilimenti in più di uno Stato membro, per stabilimento principale si intende il luogo in cui ha sede la sua amministrazione centrale nell'ambito dell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del Titolare del trattamento dati sito comunque nell'Unione e che quest'ultimo stabilimento sia la sede deputata ad assumere l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato le decisioni è considerato lo stabilimento principale;

"Stabilimento principale con riferimento a un Responsabile del trattamento dati": qualora il Responsabile del trattamento dati abbia stabilimenti in più di uno Stato membro, per stabilimento principale si intende 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 per le quali è soggetto a obblighi specifici ai sensi del GDPR;

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

3. 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 Titolare del trattamento dati è competente per il rispetto dei principi, e in grado di comprovarlo*."

3.1. Liceità, Correttezza e Trasparenza

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

3.2. Limitazione delle Finalità

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

3.3. Minimizzazione dei Dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità del trattamento. Ove possibile occorrerà procedere all'anonimizzazione o alla pseudonimizzazione dei dati personali, per ridurre eventuali rischi per gli interessati.

3.4. Esattezza

I dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure necessarie per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

3.5. 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.

3.6. Integrità e riservatezza

Considerando le tecnologie e le altre misure di sicurezza disponibili, costi di attuazione e la probabilità e gravità dei rischi per i dati personali, occorre adottare misure tecniche e organizzative per garantire un livello di sicurezza adeguato, inclusa la protezione dalla distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.

3.7. Responsabilizzazione

Compito del Titolare del Trattamento Dati è quello di assicurare e comprovare il rispetto dei principi sopra descritti.

4. Costruire la protezione dei dati nelle attività commerciali

Al fine di conformarsi ai principi che regolano la protezione dei dati, un'organizzazione dovrebbe adottare alti profili di protezione dei dati nell'espletamento delle sue attività.

4.1. Notifica agli Interessati

(Vedi Linee guida sul Corretto Trattamento.)

4.2. Scelta e Consenso dell'Interessato

(Vedi Linee guida sul Corretto Trattamento.)

4.3. Raccolta

Il detentore dei dati deve raccogliere solo i dati essenziali allo scopo del trattamento.

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

4.4. Uso, Conservazione e Smaltimento

Le finalità, i metodi, il limite di registrazione e il periodo di conservazione dei dati personali devono essere coerenti alle informazioni contenute nell'Informativa sulla Privacy. Occorre garantire 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 al fine di evitare una loro eventuale sottrazione, un utilizzo improprio o un abuso.

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

4.5. Divulgazione a terzi

Ogni volta che **Studio ZELINOTTI** 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 il terzo fornisca misure di sicurezza adeguate.

A tal fine, è necessario utilizzare il Questionario di Conformità del Responsabile del trattamento dati al GDPR.

Il Titolare del trattamento dei dati deve richiedere contrattualmente al Fornitore di fornire lo stesso livello di protezione 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 e non per altri scopi.

Quando il detentore tratta i dati personali congiuntamente con un terzo indipendente, occorre esplicitare 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.

4.6. Trasferimento Transfrontaliero dei Dati Personali

Prima di trasferire i dati personali fuori dallo Spazio Economico Europeo (SEE) devono essere utilizzate misure di protezione adeguate, tra le quali rientra la sottoscrizione di un accordo sul trasferimento dei dati, come richiesto dall'Unione Europea e, se necessario, ottenere 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.

4.7. Diritto d'Accesso da parte degli Interessati

Il Titolare del trattamento dati deve garantire agli interessati un adeguato accesso ai dati personali che li riguardano.

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.

4.8. 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 ad un altro Titolare del trattamento dati, gratuitamente e sempre esclusivamente su richiesta dell'interessato.

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

4.9. Diritto all'oblio

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

Quando il Detentore agisce come Titolare del trattamento dati, 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.

5. Linee guida sul Corretto Trattamento

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

Il titolare del trattamento dei dati 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.

5.1. 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 Titolare del trattamento dati è tenuto ad informare adeguatamente gli interessati in merito ai tipi di dati personali raccolti, alle finalità del trattamento, ai metodi di trattamento, ai diritti degli interessati riguardo ai loro dati personali, al periodo di conservazione, ai potenziali trasferimenti internazionali dei dati, se i dati saranno condivisi con terzi nonché le misure di sicurezza adottate per proteggere i dati personali.

Queste informazioni verranno fornite tramite un'Informativa sulla Privacy.

Laddove i dati personali siano condivisi con terzi, il Responsabile della Protezione dei Dati deve garantire un'adeguata informazione mediante un'Informativa sulla Privacy.

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

5.2. Ottenere i Consensi

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

Il Titolare del Trattamento è tenuto a dare agli interessati, in merito al consenso, delle opzioni informandoli circa la possibilità di revocarlo in ogni momento.

Laddove la raccolta abbia ad oggetto dati personali di un minore di anni 18, il Responsabile della Protezione dei Dati deve garantire che il consenso del Titolare della responsabilità genitoriale sia reso prima della raccolta utilizzando il modulo di consenso del Titolare della responsabilità genitoriale.

In caso di richiesta di correzione, modifica o distruzione della registrazione 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 registrare e tenere un apposito registro delle richieste.

I dati personali devono essere trattati solo per le finalità per cui sono stati originariamente raccolti. Qualora i dati personali siano raccolti per altri scopi, è necessario il consenso degli interessati in forma scritta chiara e concisa. Qualsiasi richiesta di questo tipo dovrà indicare 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.

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.

6. Organizzazione e Responsabilità

La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque abbia accesso ai dati personali trattati.

Le principali aree di responsabilità per il trattamento dei dati personali competono ai seguenti ruoli organizzativi:

Il consiglio di amministrazione o altro organo decisionale competente prende decisioni e approva le strategie generali in materia di protezione dei dati personali.

Il **Responsabile della Protezione dei Dati o qualsiasi altro dipendente competente,** è responsabile della gestione del programma di protezione dei dati personali e dello sviluppo e della promozione delle politiche di protezione dei dati personali dall'inizio alla fine del trattamento, così come definito nella Descrizione del Ruolo del Responsabile della Protezione dei Dati.

Il **Dipartimento Affari legali / il Consulente insieme al 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 i reparti del Titolare del trattamento dei dati nel raggiungimento dei loro obiettivi relativi ai dati personali.

Il **responsabile del dipartimento di Informatica** ha il compito 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.

Il **Responsabile delle Risorse Umane** ha il compito di:

- migliorare la consapevolezza di tutti i dipendenti sulla protezione dei dati personali degli utenti;

- organizzare la formazione, aumentare la competenza e la sensibilizzazione rispetto alla protezione dei dati per i dipendenti che lavorano con dati personali;
- garantire che i dati personali dei dipendenti vengano trattati in base alle legittime finalità e necessità.

Il **Responsabile degli Acquisti** è responsabile del trasferimento delle 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. Può, inoltre, chiedere un audit presso i fornitori per verificare le modalità di trattamento dei dati stessi.

7. Risposta agli incidenti di Violazione dei Dati Personali

Qualora si venisse a conoscenza di una presunta o effettiva violazione dei dati personali, occorre procedere ad 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, sarà necessario informare l'Autorità di controllo competente in materia di protezione dei dati senza indebiti ritardi e, ove possibile, entro 72 ore.

8. Audit e Responsabilizzazione

Il Responsabile della Protezione dei Dati deve verificare le modalità di implementazione di 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.

9. 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.

10. 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 Referente Privacy	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Modulo di Recesso dell'Interessato	Il Referente Privacy	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Modulo di Consenso dei Titolari della Responsabilità Genitoriale	Il Referente Privacy	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Modulo di Recesso dei Titolari della Responsabilità Genitoriale	Il Referente Privacy	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Accordi con i Fornitori del Trattamento dei Dati	Il Referente Privacy	Soltanto le persone autorizzate possono avere accesso alla cartella	10 anni dopo la scadenza del contratto
Registro delle Informative sulla Privacy	Il Referente Privacy	Soltanto le persone autorizzate possono avere accesso alla cartella	Permanente

11. Validità e gestione del documento

Questo documento ha effetto dal 08.03.2022.

Il responsabile per questo documento è il Responsabile della Protezione dei Dati, che ha il compito di controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.

02.1 - POLITICA SULLA PROTEZIONE DEI DATI PERSONALI

Codice:	02.1
Revisione:	0
Data di revisione:	
Redatto da:	Responsabile Protezione Dati
Approvato da:	Titolare del Trattamento
Livello di Riservatezza	III

Cronologia delle revisioni

Data	Revisione	Creata da	Descrizione della modifica
08.03.2022	0	DPO	Rilascio Documento