Generali Group

PERSONAL DATA PROTECTION GROUP POLICY

Versione pubblica

generali.com

RIEPILOGO

La Politica di Gruppo in materia di Dati Personali (di seguito anche la "*Group Policy*") definisce i principi di implementazione della normativa europea in materia di privacy (tra cui la GDPR - come di seguito definito -, le leggi nazionali che implementano le previsioni della GDPR e le linee guida emanate dal European Data Protection Board) in tutto il Gruppo e stabilisce i requisiti minimi che ciascuna Società del Gruppo deve applicare quando tratta Dati Personali.

A questo fine, la Politica prevede:

- i principi che devono ispirare il Trattamento dei Dati Personali;
- i requisiti chiave da implementare a seconda che si agisca nella qualità di Titolare del Trattamento, Responsabile del Trattamento o Contitolare del Trattamento con riferimento ad uno specifico Trattamento dei Dati Personali.

INDICE

1. Introduzione

1.1 OBIETTIVI

Il Gruppo Generali considera la salvaguardia dei Dati Personali come una priorità per proteggere i diritti fondamentali e le libertà dei clienti, dei dipendenti e di tutti gli altri *stakeholder*.

Lo scopo della Politica di Gruppo in materia di Dati Personali è di definire i principi chiave e i requisiti fondamentali da seguire quando sono trattati i Dati Personali tenendo conto delle previsioni del GDPR.

Questa Politica definisce anche i ruoli chiave da coinvolgere per la gestione dei rischi associati al Trattamento dei Dati Personali.

2. Principi generali nel Trattamento dei Dati Personali

I seguenti principi generali devono essere sempre applicati al Trattamento dei Dati Personali:

- **liceità, correttezza e trasparenza**: identificare per ciascun Trattamento un presupposto legittimante ("base giuridica") valido e fornire all'Interessato un'Informativa appropriata. Il Trattamento indebito, inatteso o fuorviante dei Dati Personali non è ammesso;
- **limitazione della finalità:** trattare i Dati Personali solo per finalità determinate, esplicite e legittime, così come descritte nell'Informativa. Trattamenti ulteriori incompatibili con le finalità dichiarate non sono ammessi;
- **minimizzazione:** trattare solo i dati necessari per perseguire le finalità descritte nell'Informativa;
- **accuratezza**: non trattare Dati Personali inesatti od errati e, quando necessario, aggiornali; quando si verifica che un Dato Personale sia inesatto o errato rispetto alle finalità per cui trattato, le Società del Gruppo devono adottare tutte le misure ragionevoli per correggerli o cancellarli tempestivamente;
- **limitazione della conservazione**: conservare i Dati Personali per il tempo necessario al perseguimento delle finalità per le quali sono trattati; definire il periodo di conservazione dei dati. Il periodo di conservazione dei dati varia a seconda dello scopo del Trattamento con il limite del rispetto delle altre fonti normative. Trascorso il periodo di conservazione, i Dati Personali possono essere conservati solo se non consentono l'identificazione dell'Interessato. Per garantire il rispetto di questo principio devono essere adottate misure tecniche che de-identifichino in modo irreversibile i Dati Personali, quali ad esempio la cancellazione, l'offuscamento, la redazione, l'anonimizzazione;
- **integrità e confidenzialità**: assicurare che appropriate misure tecnico e organizzative siano implementate al fine di proteggere i Dati Personali così da evitare Trattamenti non autorizzati, illeciti, perdite accidentali, distruzione o danneggiamento.

Il Titolare del Trattamento è responsabile per il rispetto dei suddetti principi e deve essere in grado di dimostrare in ogni momento (principio di **"responsabilizzazione**") la conformità, attraverso l'adozione di normativa interna, processi ed altre misure adeguate, che possono includere almeno la tenuta del registro dei Trattamenti, lo svolgimento della DPIA e lo svolgimento di controlli che verifichino lo stato di implementazione dei principi e requisiti in materia di protezione dei Dati Personali.

3. Requisiti chiave

Tenendo in considerazione i suddetti principi, diversi requisiti chiave devono essere implementati a seconda che i Dati Personali siano trattati da una Società del Gruppo in qualità di Titolare, di Responsabile o di Contitolare del trattamento.

Il Titolare del Trattamento e il Responsabile del Trattamento devono fornire al personale che tratta i Dati Personali istruzioni e formazione appropriate per assicurare che i Dati Personali siano trattati in conformità con la presente *Group Policy* e alle norme tempo per tempo vigenti.

3.1 REQUISITI CHIAVE PER IL TITOLARE DEL TRATTAMENTO

Ogniqualvolta, con riferimento a uno specifico Trattamento di Dati Personali, le Società del Gruppo agiscono in qualità di Titolari del Trattamento le attività elencate nella presente Sezione devono essere eseguite.

Il Titolare deve comunque garantire che il Responsabile dei Dati Personali, quando nominato, venga prontamente e per tempo coinvolto (sin dalla fase iniziale) quando una attività abbia a che fare con il Trattamento di Dati Personali.

3.1.1 Trattare i Dati Personali sulla base di un presupposto legittimante

Il Titolare deve identificare una base legittima per il Trattamento prima che il Trattamento sia iniziato.
L'identificazione del corretto presupposto legittimante dipende dallo scopo e dalla natura di relazione con Interessati coinvolti (ad es. dipendenti, clienti, altri interlocutori) e la natura dei Dati Personali, in particolare se Categorie Particolari di Dati Personali sono trattati.

Il Trattamento è legale quando è:

- basato sul consenso prestato dall'Interessato per una o più specifiche finalità; o
- necessario per l'esecuzione di: (i) un contratto di cui è parte l'Interessato o (ii) misure precontrattuali adottate su richiesta dello stesso Interessato; o
- necessario per adempiere un obbligo legale al quale è soggetto la Società del Gruppo; o
- necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica; o
- necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento; o
- necessario per il perseguimento di un legittimo interesse da parte della Società del Gruppo, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei Dati Personali.

Il Trattamento di Categorie Particolari di Dati Personali è vietato, eccetto quando si verifica uno dei seguenti casi:

- è basato sul consenso esplicito dato dall'Interessato per una o più finalità specifiche, salvo nei casi in cui la normativa applicabile dispone che l'Interessato non possa revocare il divieto;
- è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del Trattamento o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dalla normativa applicabile;
- è necessario per tutelare un interesse vitale dell'Interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base della normativa applicabile o conformemente al contratto con un professionista della sanità, fatte salve le seguenti condizioni e garanzie: tali Dati Personali sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente alla normativa applicabile o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente alla normativa applicabile;
- è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
- effettuato in conformità con la normativa applicabile, comprese ulteriori condizioni e limitazioni, con riguardo al Trattamento di Categorie Particolari di Dati Personali.

3.1.2 Fornire agli Interessati appropriate informazioni relative al Trattamento dei Dati Personali

Il Titolare del Trattamento deve rilasciare agli Interessati una chiara e completa Informativa sul trattamento dei Dati Personali che si appresta a svolgere.

L'Informativa deve essere concisa, trasparente, accessibile e intellegibile. Deve essere scritta in modo facile da comprendere.

Il Titolare del Trattamento, prima dell'implementazione o rilascio di una nuova Informativa, o modifica di una esistente, deve consultare il DPO sulla nuova o modificata informativa prima della finalizzazione della stessa. Il DPO deve controllare che il suo contenuto sia accurato e corrispondente al registro dei Trattamenti dei Dati Personali e che tutte le attività rilevanti di Trattamento dei Dati Personali della Società del Gruppo siano incluse.

3.1.3 Facilitare l'esercizio dei diritti degli Interessati

Come regola generale ed a certe condizioni definite dalle normative applicabili, il Titolare deve garantire che gli Interessati esercitino liberamente i seguenti diritti sui propri dati personali:

a) **diritto di accesso**: diritto di ottenere la conferma che sia o meno in corso un Trattamento dei Dati Personali che lo riguardano e, in tal caso, ottenere l'accesso ai Dati Personali senza indebito ritardo;
b) **diritto di rettifica**: diritto di ottenere, senza indebito ritardo, la rettifica dei Dati Personali inesatti;
c) **diritto di cancellazione (diritto all'oblio)**: diritto di ottenere, senza indebito ritardo, la cancellazione dei Dati Personali da qualsiasi supporto su cui siano archiviati;

d) **diritto di limitazione di trattamento**: diritto di ottenere la limitazione delle attività di trattamento sui Dati Personali degli Interessati. Una volta limitati, i Dati Personali possono essere solo conservati, eccezion fatta per casi specifici;
e) **diritto alla portabilità**: il diritto degli Interessati a ricevere i propri Dati Personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, nonché di trasmettere tali Dati Personali ad altro Titolare del Trattamento;
f) **diritto di opporsi**: il diritto di opporsi in qualsiasi momento al Trattamento dei Dati Personali degli Interessati per motivi connessi alla loro situazione specifica. Una volta esercitato il diritto di opposizione, i Dati Personali non devono più essere trattati a meno che non si dimostri l'esistenza di ragioni legittime prevalenti rispetto agli interessi, diritti e libertà degli Interessati, o la necessità di accertare, esercitare o difendere un diritto in sede giudiziaria. In ogni caso, se gli Interessati si oppongono al trattamento per finalità di marketing diretto, i Dati Personali non devono più essere trattati a tali fini;
g) **diritto a non essere sottoposto a una decisione basata unicamente sul Trattamento automatizzato**: il diritto dell'Interessato a non essere sottoposto a una decisione basata unicamente sul Trattamento automatizzato, inclusa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

In particolare il Titolare deve:

- definire un processo che consenta l'agevole esercizio dei diritti degli Interessati ed adottare prontamente le azioni necessarie;
- informare gli Interessati sulle azioni intraprese;
- informare gli Interessati sulle modalità attraverso cui poter esercitare tali diritti.

Salvo che si verifichino circostanze eccezionali, tutte le attività e le comunicazioni agli Interessati devono essere rese a titolo gratuito per gli Interessati.

3.1.4 Garantire l'adozione di un approccio *by design* e *by default* alla protezione dei Dati Personali

Il Titolare deve garantire il rispetto del principio alla protezione dei Dati Personali *by design* e *by default*.

Il Titolare deve identificare ed implementare appropriate misure tecnico organizzative utili a garantire il rispetto dei requisiti del GDPR ed a proteggere i diritti e le libertà degli Interessati; quanto sopra deve avvenire già al tempo della determinazione degli scopi e dei mezzi del Trattamento, sia che questo avvenga nell'ambito di un sistema, di un servizio, di un prodotto oppure di un processo (**privacy by design**).

Per l'identificazione delle misure tecnico e organizzative appropriate, il Titolare deve prendere almeno in considerazione quanto segue:

- le soluzioni tecniche e tecnologiche disponibili sul mercato in quel momento,
- il costo di implementazione,
- la natura, il contenuto, il contesto e lo scopo del Trattamento dei Dati Personali,
- gli impatti del Trattamento sui diritti e le libertà degli Interessati.

Misure tecnico e organizzative appropriate devono garantire *by default* che siano trattati i soli Dati Personali necessari per la specifica finalità; lo stesso principio vale con riferimento alla quantità di Dati Personali raccolti, all'estensione del Trattamento, al loro periodo di conservazione ed alla loro accessibilità (***privacy by default***).

4.1.5 Tenere il registro dei Trattamenti svolti sotto la propria responsabilità

Il Titolare del Trattamento deve tenere un registro dei Trattamenti dei Dati Personali e curare che sia pronto per essere reso disponibile alle autorità di controllo.

4.1.6 Implementare misure tecnico e organizzative adeguate a garantire un livello di sicurezza dei Dati Personali commisurato al rischio

Il Titolare deve implementare misure tecnico e organizzative adeguate così da garantire un livello di sicurezza dei Dati commisurato al rischio.

Un approccio *risk- based* deve essere utilizzato nella identificazione delle predette misure. L'approccio deve quantomeno tenere in considerazione, tra i vari fattori, il livello di sviluppo della tecnologia, la natura, il contenuto, il contesto, lo scopo e l'impatto

potenziale in termini di probabilità e gravità delle conseguenze sui diritti e libertà degli Interessati del Trattamento.

Il Titolare, con un approccio *by design* e by *default*, consulta il DPO anche sugli aspetti relativi alle misure tecnico e organizzative da implementare fermo restando il coinvolgimento di ogni altra funzione in relazione alla propria area di responsabilità.

4.1.7 Notificare alla autorità di controllo e comunicare agli Interessati una violazione dei Dati Personali

Il Titolare deve implementare un processo che assicuri una adeguata gestione delle violazioni dei Dati Personali.

Il processo deve prevedere il coinvolgimento del DPO, se nominato, e una tempestiva notifica delle violazioni dei Dati Personali all'autorità di controllo entro e non oltre le 72 ore dal momento in cui se ne è venuti a conoscenza, a meno che sia improbabile che la violazione dei Dati Personali presenti un rischio per i diritti e le libertà degli Interessati e, ove rilevante, la comunicazione agli Interessati impattati.

4.1.8 Svolgere la Valutazione di Impatto sulla Protezione dei Dati Personali *(DPIA)*

Al verificarsi di determinate circostanze, il Titolare deve svolgere la Valutazione di Impatto sulla Protezione dei Dati Personali (*DPIA*).

Gli obiettivi della *DPIA* sono:

- descrivere il Trattamento dei Dati Personali;
- valutare la necessità e la proporzionalità del Trattamento rispetto alle relative finalità; e
- contribuire a gestire i rischi per i diritti e le libertà degli Interessati che possano sorgere in relazione a tale Trattamento.

Il Titolare consulta il DPO, quando nominato svolge la valutazione di impatto, nello svolgimento della DPIA.

4.1.9 Adottare misure adeguate per il trasferimento di Dati Personali al di fuori dello Spazio Economico Europeo (SEE)

Il Titolare deve garantire che il trasferimento di Dati Personali al di fuori delle dello Spazio Economico Europeo (SEE) sia posto in essere solo ove necessario e solo dopo aver adottato almeno una delle salvaguardie consigliate e le misure supplementari appropriate per assicurare che i Dati Personali trasferiti ricevano, nel paese di destinazione non SEE, un livello di protezione sostanzialmente equivalente a quello fornito nel SEE. La preferenza deve essere comunque data a Trattamenti che si svolgono all'interno del SEE.

La preferenza deve essere data alle salvaguardie nel seguente ordine:

- il paese non appartenente allo SEE garantisce un livello adeguato di protezione dei Dati Personali sulla scorta della valutazione della Commissione Europea; o
- il trasferimento è necessario per l'esecuzione di un contratto tra il Titolare del Trattamento e l'Interessato; o
- il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; o
- l'Interessato ha prestato il consenso esplicito al trasferimento dei Dati Personali; o
- le clausole standard di protezione dei Dati Personali adottate dalla Commissione Europea sono adempiute e possono essere pienamente implementate (alla luce delle leggi e pratiche dei paesi non appartenenti allo SEE di destinazione dei Dati Personali); o
- come ipotesi residuale, quando il trasferimento non è sistematico e riguarda solo un numero limitato di Interessati, è necessario per perseguire l'interesse legittimo della Società del Gruppo, a condizione che: siano state valutate tutte le circostanze e il Titolare abbia adottato tutte le garanzie necessarie per il Trattamento e l'autorità di controllo sia stata debitamente informata del trasferimento.

Quando il trasferimento ad un paese non SEE è basato sulle clausole standard di protezione dei Dati Personali **adottate dalla** Commissione Europea, il Titolare deve valutare se sono effettive considerando tutte le circostanze del trasferimento e, se no, il titolare deve adottare misure addizionali (come la crittografia "*in transit*" e "*at rest*", la crittografia "*end-to-end"*, l'anonimizzazione, la pseudonimizzazione) al fine di assicurare che i Dati Personali trasferiti siano riconosciuti nel paese terzo un livello di protezione essenzialmente equivalente a quello garantito nell'Unione Europea.

Se nessuna salvaguardia è applicabile e/o nessuna misura addizionali sembra essere efficace ad assicurare che i Dati Personali trasferiti ricevano, nel paese terzo di destinazione, un livello di protezione essenzialmente equivalente a quello garantito nell'Unione Europea, o nel caso di dubbio, il Titolare deve astenersi dal trasferire Dati Personali.

Le previsioni sul trasferimento di Dati Personali si applicano sia trasferimenti di Dati Personali nel Gruppo che al di fuori del Gruppo (e.g., fornitori, venditori).

4.1.10 Nominare un Responsabile del trattamento dei dati

Quando il Titolare delega il Trattamento dei Dati Personali ad un terzo (all'interno o all'esterno del Gruppo), il Titolare deve nominare il Responsabile del trattamento per iscritto. La nomina deve essere formalizzata anche quando si verifica nell'ambito di un contratto di esternalizzazione, conformemente alla Outsourcing Group Policy.

Prima che un Responsabile del Trattamento sia nominato, il Titolare deve verificare che il Responsabile abbia in essere misure tecnico e organizzative appropriate per garantire la conformità ai principi e requisiti in materia di protezione dei Dati Personali nonché l'esercizio dei diritti da parte degli Interessati. Il Titolare deve autorizzare qualsiasi nomina da parte del Responsabile del Trattamento di un altro Responsabile del Trattamento. L'autorizzazione preliminare scritta può essere generica o specifica.

3.2 REQUISITI CHIAVE PER IL RESPONSABILE DEL TRATTAMENTO

Ogniqualvolta, in relazione ad una specifica operazione di Trattamento di Dati Personali, la Società del Gruppo agisce in qualità di Responsabile del trattamento, deve:

- trattare i Dati Personali in conformità ai principi della presente *Group Policy,* delle leggi e dei regolamenti applicabili in materia di protezione dei Dati Personali e solo sulla base delle istruzioni fornite dal Titolare, salva diversa previsione delle leggi applicabili;
- assicurarsi che i soggetti autorizzati a trattare i Dati Personali si siano impegnati ad agire con riservatezza o siano tenuti ad un appropriato obbligo di riservatezza;
- mantenere un registro di tutte le attività di Trattamento;
- implementare adeguate misure tecniche e organizzative per proteggere il Trattamento dei Dati Personali;
- in caso di trasferimento dei Dati Personali al di fuori dello SEE, applicare le salvaguardie e le misure come descritte in questa *Group Policy*;
- firmare un contratto o altro atto giuridico che disciplini la relazione con il Titolare del Trattamento;
- astenersi dal nominare un altro Responsabile del trattamento senza la previa autorizzazione specifica del Titolare del Trattamento. Nel caso in cui il Responsabile del Trattamento abbia ricevuto per iscritto un'autorizzazione generale per nominare altri Responsabili, deve informare tempestivamente il Titolare di eventuali modifiche che intenda apportare con riferimento alla nomina o alla sostituzione di altri Responsabili al fine di dare al Titolare del Trattamento l'opportunità di opporsi a tali modifiche;
- ogni qual volta il Responsabile del trattamento si avvalga di altri Responsabili per l'esecuzione di specifiche attività di trattamento per conto del Titolare del Trattamento, sottoscrivere un contratto con questo nuovo Responsabile al fine di imporgli gli stessi obblighi di protezione dei Dati Personali previsti nel contratto con il Titolare del Trattamento;
- supportare il Titolare del Trattamento in relazione agli obblighi in materia di riscontro alle richieste di esercizio dei diritti da parte degli Interessati;
- supportare il Titolare del Trattamento nell'adempimento delle proprie obbligazioni cooperando tempestivamente nel processo di DPIA effettuato dal Titolare e nell'eventuale previa consultazione con l'autorità di controllo competente;
- fornire notifica immediata al Titolare del Trattamento in relazione a qualsiasi Violazione di Dati Personali o incidenti che coinvolgano Dati Personali trattati per conto del Titolare del Trattamento;
- terminata la prestazione dei servizi, cancellare le copie esistenti di Dati Personali, su richiesta del Titolare del Trattamento, a meno che la legislazione dell'Unione Europea o dello Stato membro richieda la conservazione di tali Dati Personali;
- mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di legge in qualità di Responsabile del Trattamento e collaborare nelle attività di controllo, ivi incluse le ispezioni, effettuate dal Titolare del Trattamento o da altro revisore nominato dal Titolare del Trattamento.

3.3 REQUISITI CHIAVE DEI CONTITOLARI

Quando due o più Titolari agiscono come Contitolari (sia all'interno che all'esterno del Gruppo), ciascun Contitolare parte dell'accordo di contitolarità, prima della firma dello stesso, deve:

- verificare che l'altro\i Contitolare\i abbia\no implementato adeguate misure tecnico e organizzative così da garantire l'applicazione conforme della normativa, interna ed esterna, in materia di Protezione dei Dati Personali;
- stipulare un accordo che, almeno, definisca le rispettive responsabilità per la conformità con la normativa in materia di Dati Personali, in particolare con riferimento:

- alla individuazione delle responsabilità in merito alla osservanza degli obblighi normativi interni ed esterni,
- agli obblighi di trasparenza,
- allo svolgimento della DPIA, alla tenuta del registro dei Trattamenti ed alla gestione delle Violazioni dei Dati Personali,
- al punto di contatto con gli Interessati;
- al trasferimento dei Dati Personali (se previsto).

L'accordo deve essere formalizzato per iscritto e i suoi elementi essenziali devono essere messi a disposizione degli Interessati.