Gruppo Generali

Disposizioni Attuative del Codice di Condotta

Dati personali e privacy

Titolo		Disposizioni Attuative del Codice di Condotta Dati personali e privacy
Emanato da		Group CEO
	Società	Assicurazioni Generali S.p.A.
	Paese	Mondo
Destinatari		Il Personale, come definito dal Codice di Condotta
Referente	*Nome*	Group Compliance
	e-mail	GroupCompliance@Generali.com

Principali documenti correlati
Codice di Condotta e sue Disposizioni Attuative

Data 30/01/2014

Firma *M.Greco*

1. Introduzione

Il Gruppo tratta[1] regolarmente Dati Personali (di dipendenti, clienti, danneggiati, clienti potenziali o candidati, ecc.) ed adotta le misure necessarie a garantire la loro sicurezza e protezione.

Per Dati Personali si intendono le informazioni attinenti ad un individuo identificato o identificabile, come ad esempio indirizzo, numero di passaporto o di carta d'identità, stato di salute o di famiglia, coordinate bancarie, ecc.

Le presenti Disposizioni Attuative definiscono le regole fondamentali da osservare in caso di trattamento di Dati Personali nell'ambito delle Compagnie del Gruppo e trovano applicazione con riferimento a tutte le informazioni idonee a identificare, direttamente o indirettamente, una persona fisica (Interessato), siano esse conservate in formato elettronico o cartaceo.

Specifici paesi possono richiedere l'applicazione, a livello locale, di ulteriori norme più stringenti; è possibile consultare il proprio Privacy Officer per ogni informazione in merito.

2. Principi generali

Nel trattare Dati Personali, è necessario adeguarsi ai seguenti principi fondamentali:

a. *I Dati Personali devono essere trattati secondo la legge e in modo corretto e trasparente nei confronti dell'Interessato.*

   I Dati Personali vanno trattati in conformità a quanto previsto dalla normativa applicabile, sia esterna che interna.

b. *I Dati Personali devono essere raccolti per finalità specifiche, esplicite e legittime.*

   I Dati Personali devono essere raccolti e utilizzati solo per ragioni legittime, da esplicitarsi all'Interessato, e non possono essere trattati in modo incompatibile rispetto ad esse.

   Ad esempio, i Dati Personali raccolti per scopi connessi ai sinistri non possono essere utilizzati per finalità di marketing.

c. *I Dati Personali possono essere divulgati solo se strettamente necessario in relazione alle specifiche esigenze lavorative*

   E' consentito condividere Dati Personali solo nei casi in cui sia strettamente necessario (sulla base di quanto indicato al punto b).

   Per esempio, non è generalmente consentita la condivisione di Dati Personali con altre società ovvero la loro diffusione pubblica, compresa la condivisione attraverso social networks.

d. *I Dati Personali devono essere adeguati, pertinenti e limitati a quanto strettamente necessario rispetto agli scopi per i quali sono trattati*

   Possono essere raccolti solo i Dati Personali di cui la Società ha bisogno al fine di fornire il servizio richiesto dall'Interessato.

   Per esempio, se i Dati Personali sono necessari per gestire la liquidazione di una polizza vita, non devono essere raccolte informazioni relative alle convinzioni religiose od alle opinioni politiche, in quanto generalmente irrilevanti ai fini della liquidazione.

e. *I Dati Personali devono essere sempre corretti e aggiornati*

   I Dati Personali conservati dalla Società devono essere attendibili e non fuorvianti.

[1] Per trattamento si intende ogni operazione legata alla raccolta, registrazione, conservazione o cancellazione dei dati personali.

Occorre adottare ogni misura ragionevole per assicurare che i Dati Personali non corretti (avuto riguardo degli scopi per i quali sono trattati) siano cancellati o rettificati senza ritardo.
Se l'Interessato chiede un aggiornamento dei propri Dati Personali, alla richiesta va dato seguito senza ritardo.

f. I Dati Personali devono essere cancellati o mantenuti in un formato che non consenta l'identificazione dell'Interessato, una volta che sia stato ottenuto lo scopo per cui essi sono stati raccolti

I Dati Personali devono essere mantenuti solo per il tempo ragionevolmente necessario.
Per esempio, i Dati Personali relativi a candidati che non abbiano superato il processo di selezione del personale, non possono essere conservati per un periodo superiore a qualche mese rispetto al momento della loro candidatura.

g. Diritti dell'Interessato

All'Interessato deve essere garantito il diritto ad accedere ai propri Dati Personali, nonché il diritto di ottenere la rettifica, il blocco, la cancellazione o la distruzione dei dati non corretti.

3. Trattamento dei Dati Personali

3.1 Informazioni da fornire all'Interessato

Al fine di rendere gli Interessati consapevoli delle modalità con cui i loro Dati Personali saranno trattati e con cui essi potranno esercitare i propri diritti, nel momento della raccolta dei Dati, occorre fornire loro le seguenti informazioni:

- I dati identificati e i contatti della Società;
- Le finalità del trattamento per cui i Dati sono raccolti;
- I soggetti (o le categorie di soggetti) a cui i Dati sono comunicati e le finalità del trasferimento;
- La natura obbligatoria o facoltativa del conferimento dei Dati e le conseguenze derivanti dal rifiuto di fornire le informazioni, o, quando richiesto, il consenso;
- Il loro diritto di ottenere l'accesso, la rettifica o la cancellazione dei propri Dati Personali;
- Il loro diritto di opporsi al trattamento dei propri Dati Personali[2] e le relative conseguenze;
- Ove applicabile, il diritto di sporgere reclamo all'Autorità competente in materia di privacy ed i relativi contatti;
- Le modalità con cui avanzare eventuali richieste di accesso ai Dati Personali e le persone/strutture responsabili per rispondere a tali richieste;
- La possibilità che i Dati Personali siano trasferiti a società situate all'estero e il livello di protezione offerto.

Il Privacy Officer[3] competente elabora lo *standard* di informativa privacy avente gli anzidetti contenuti e definisce le fattispecie in cui essa debba essere utilizzata. Sulla base di quanto previsto dalla normativa applicabile, il Privacy Officer stabilisce altresì i casi in cui l'anzidetta informativa può essere fornita oralmente e quelli in cui deve essere fornita per iscritto.

[2] Quando richiesto dalla normative o regolamentazione applicabile a livello locale.

[3] Cfr. il successivo par. 4.1.

3.2 Consenso dell'Interessato

E' di norma necessario richiedere il consenso dell'Interessato alla raccolta dei suoi Dati Personali. Sulla base di quanto previsto dalla normativa locale applicabile, il Privacy Officer definisce i casi in cui il consenso deve essere richiesto e se esso va prestato oralmente o per iscritto.

Il consenso scritto è sempre necessario se i Dati Personali richiesti sono idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o di altro genere ovvero l'appartenenza ad un'organizzazione sindacale, nonché in caso di dati genetici ovvero di dati attinenti la salute o la vita sessuale, le condanne penali o correlate misure di sicurezza.

3.3 Richieste dell'Interessato

Agli Interessati deve essere garantito il diritto, senza limitazioni, di chiedere alla Società:

- La conferma dell'esistenza di propri Dati Personali presso la Società;
- L'indicazione dei soggetti o delle categorie di soggetti cui i Dati Personali possono essere comunicati;
- La cancellazione, la trasformazione in forma anonima o il blocco dei Dati Personali trattati illecitamente;
- La rettifica, il blocco, la cancellazione o la distruzione dei Dati Personali non corretti.

Le richieste vanno riscontrate senza ritardo, dopo aver verificato l'identità del richiedente.

Va chiaramente individuato almeno un manager responsabile per il riscontro delle richieste provenienti dagli Interessati.

3.4 Uso dei Dati Personali per finalità di marketing

La volontà dell'Interessato che neghi o ritiri il proprio consenso all'uso dei propri Dati Personali per finalità di marketing (comunicazioni promozionali e commerciali) va rispettata. La Società adotta a tal fine appropriate iniziative, quali, ad esempio, la creazione di una lista di Interessati che non devono essere contattati per finalità di marketing, da trasmettere alla rete di vendita.

3.5 Trasferimento di Dati Personali

Spesso si pone l'esigenza di trasferire Dati Personali, compresi quelli dei dipendenti, nell'ambito del Gruppo od a soggetti terzi.

I Dati Personali devono essere trasferiti solo se strettamente necessario. Il trasferimento deve essere regolato da un accordo scritto tra la società cedente e la ricevente, salvo che il trasferimento sia altrimenti consentito dalla legge o dalla normativa locale.

Nei casi in cui i Dati Personali debbano essere trasferiti all'estero, prima del trasferimento occorre valutare il livello di protezione dei Dati assicurato dal paese ricevente. Qualora il paese ricevente non dovesse offrire un adeguato livello di protezione dei Dati Personali, il trasferimento potrà avvenire solo a condizione che l'Interessato abbia prestato il proprio consenso informato[4] ovvero la protezione dei Dati sia stata regolata mediante clausole contrattuali standard.

Il Privacy Officer definisce i casi in cui i Dati Personali possono essere legittimamente trasferiti.

3.6 Outsourcing

In tutti i casi in cui la Società decida di ricorrere all'outsourcing, il Privacy Officer dovrà verificare che l'outsourcer operi in conformità alle presenti Disposizioni Attuative per quanto attiene al trattamento di Dati Personali per conto del Gruppo.

In ogni caso, la responsabilità ultima rispetto al trattamento dei Dati Personali rimane in capo alla Società.

[4] L'interessato deve essere consapevole che ai propri Dati Personali potrebbe non essere offerto lo stesso livello di protezione riconosciuto dalla società a cui i Dati sono stati forniti.

4. Misure attuative

Ogni società del Gruppo deve definire e documentare adeguatamente le modalità e le finalità del trattamento dei Dati Personali.

A tal fine, ogni Società deve porre in essere almeno le seguenti misure attuative.

4.1 Ruoli

4.1.1 Privacy Officer

Ciascuna Società del Gruppo individua un Privacy Officer con la responsabilità di sovrintendere al rispetto delle presenti Disposizioni Attuative.

Il Privacy Officer deve essere in possesso di adeguate competenze ed esperienza con riferimento alla normativa applicabile in materia di protezione dei Dati Personali. Eventuali ulteriori responsabilità in ambito aziendale devono essere compatibili con quelle derivanti dall'incarico di Privacy Officer. A meno dell'esistenza di conflitti di interesse, il Privacy Officer può coincidere con il Compliance Officer della Società o, tenuto conto della dimensione della Società, l'incarico può essere affidato in outsourcing ad un'altra società del Gruppo.

4.1.2 Manager

La Società identifica uno o più manager incaricati di assicurare che i propri dipendenti ricevano adeguate istruzioni su come applicare le disposizioni in materia di privacy nella loro attività lavorativa quotidiana nonché di monitorarne il rispetto nell'ambito della propria area di responsabilità.

4.2 Sicurezza

4.2.1 Sicurezza dei documenti cartacei ed elettronici

La Società archivia e controlla i Dati Personali con l'obiettivo di minimizzare i rischi di distruzione, perdita accidentale, accessi non autorizzati o trattamenti che esulano dalle finalità per le quali sono stati raccolti.

4.2.2 Accesso ai Dati Personali da parte dei dipendenti

La Società assicura che i propri dipendenti abbiano accesso ai database ed agli archivi della Società ed ai dati Personali ivi contenuti limitatamente a quanto richiesto dai compiti e dalle mansioni svolte.

4.3 Mappatura dei trattamenti

La Società mantiene e aggiorna regolarmente una mappa dei trattamenti, nella quale sono contenute informazioni di dettaglio circa il flusso dei Dati Personali in entrata ed in uscita nonché i manager responsabili dei relativi trattamenti.

La mappa dei trattamenti deve consentire l'agevole reperimento della correlata documentazione alle autorità od al personale autorizzato che ne faccia richiesta.

4.4 Conseguenze delle violazioni

Il Gruppo può essere considerato responsabile di eventuali trattamenti illeciti di Dati Personali.

Oltre al potenziale onere finanziario derivante dalla condanna al pagamento di una multa, eventuali violazioni potrebbero comportare danni reputazionali per il Gruppo.

5. Responsabilità

Il **CEO** è responsabile di assicurare che:

- Le presenti Disposizioni Attuative vengano adottate;
- Siano definite le finalità di trattamento dei Dati Personali;
- I Dipendenti ricevano un'adeguata formazione circa gli adempimenti in materia di privacy correlati al ruolo ricoperto;

- Sia individuato almeno un manager responsabile per il riscontro delle richieste da parte degli Interessati.

La funzione **Group Compliance di Assicurazioni Generali** è responsabile per:

- rivedere periodicamente e mantenere le presenti Disposizioni Attuative,
- fornire consulenza e monitorare l'adozione delle Disposizioni.

Il **Privacy Officer** è responsabile per :

- Supportare e fornire consulenza sulle presenti Disposizioni Attuative;
- Monitorare l'evoluzione della normativa in materia di protezione dei dati personali ed elaborare linee guida sulla sua corretta attuazione;
- fornire consulenza sugli adempimenti in materia di sicurezza dei dati;
- elaborare linee guida sull'informativa sul trattamento dei Dati Personali da rendere agli Interessati e sui casi in cui va richiesto il consenso;
- Definire i casi in cui il trasferimento dei Dati Personali può considerarsi legittimo.

I **manager** sono responsabili per :

- assicurare che i dipendenti ricevano specifiche istruzioni sul corretto trattamento dei Dati Personali;
- monitorare il trattamento dei Dati Personali;
- mantenere ed aggiornare regolarmente la mappa dei trattamenti.