Regolamento sulla Privacy

Note e azioni da intraprendere

Il nuovo regolamento sulla privacy è entrato in vigore il 25 maggio, ma in verità rappresenta l'attuazione di una direttiva comunitaria risalente al 2016. Fortunatamente l'Italia era già abbastanza al passo con la sua cara vecchia normativa, per cui già qual poco che avevamo attuato come associazione si è rivelato essere un buon inizio. Ciò nonostante, si sono rivelate necessarie alcune azioni correttive (già intraprese) e sarebbero opportuni alcuni ulteriori adempimenti.

Note:

Livello di priorità

Nel considerare l'importanza e la priorità di tali adempimenti, è necessario considerare lo scopo primo della normativa: regolamentare le attività di profilazione della clientela e la compravendita di dati personali da parte di **grosse aziende**, che operano a **fini di lucro**. Ciò non invalida la necessità di tali adempimenti, ma sicuramente la mette in secondo piano rispetto ad altri nostri obiettivi, almeno dal punto di vista normativo.

Definizione di Trattamento dei Dati

Nel riflettere sui nostri processi di utilizzo dei dati degli associati e delle altre persone con cui veniamo in contatto, è importante che teniamo bene a mente cosa è e cosa non è "trattamento":

- **Rappresenta trattamento dei dati** la raccolta di dati comuni e/o sensibili a fini:
  - promozionali,
  - di creazione di un profilo statistico della persona.
- **Non rappresenta** trattamento dei dati la richiesta di dati per portare a termine un'operazione una tantum (es: chiedere nome e numero di telefono per invitare qualcuno a un evento particolare).

Si noti che ogni volta che i dati di una persona vengono raccolti in una base dati informatica, ci sono i presupposti per un uso "promozionale", per cui è necessario informare adeguatamente gli interessati sull'uso che se ne intende fare.

Adempimenti obbligatori

L'unico adempimento realmente obbligatorio è far prendere visione agli interessati dell'informativa. Il consenso non è obbligatorio, in quanto se l'interessato ha letto l'informativa e fornisce i dati, sta fornendo un consenso implicito.

L'informativa deve esplicitare:

- chi tratta i dati,
- come,
- perché e
- quali sono i diritti dell'interessato.

L’informativa deve essere scritta:

- in un linguaggio chiaro e accessibile,
- senza scritte in piccolo,
- possibilmente e preferibilmente online.

L’informativa deve essere fornita:

- per intero, a soli fini consultativi e
- nello specifico, quando uno usufruisce di un singolo servizio. È necessario allora produrre un estratto comodo da leggere dell’intera normativa, relativo solo ad alcuni aspetti dell’intero trattamento (es: chiedere l’indirizzo e-mail per commentare sul sito).

Per acquisire i dati dell’interessato occorre che sussista una base giuridica valida. Si intenda questa come un motivo valido dal punto di vista giuridico per richiedere quel dato specifico. Questo deve essere esplicitato nell’informativa, a meno che sia una motivazione in termini di legge (es: alcuni dati dell’associato devono essere forniti per inserirlo nel libro soci).

Se non c’è un’effettiva necessità di acquisire alcuni dei dati dell’interessato, la normativa impone di non acquisirli.

Basi del trattamento dati = Principi importanti da conoscere

Si riportano qui i principi base su cui poggia il decreto. Essi sostituiscono in parte le linee guida che venivano “tradizionalmente” fornite dalla normativa italiana sulla privacy:

- **Accountability = responsabilizzazione**: significa che il Responsabile del trattamento ha la piena responsabilità del modo in cui essi vengono trattati. Non esistono modalità da seguire in modo ferreo, non sono definiti standard per cui il Responsabile è libero di disegnare i processi di trattamento come meglio crede. Se si verificano problematiche legate al trattamento dei dati, la responsabilità ricade in toto sul Responsabile.
- **Data Protection by Design**: il processo di trattamento deve prevedere fin dalla sua concezione le scelte corrette per la protezione dei dati e la trasparenza.
- **Data Protection by Default**: ci si deve fornire di regole minime ma efficaci, per evitare rischi alla sicurezza dei dati.
- **Notifica di Data Breach**: se avviene un evento che fa temere per la sicurezza dei dati, è obbligatorio avvisare **il Garante** e **gli interessati** entro 72 ore.
- **Documentazione**: organigramma, valutazione dell'impatto, analisi dei rischi, procedure ben definite, lettere d'incarico, registro attività di trattamento.
  Non obbligatoria nel nostro caso!
- **Informativa Leggibile**
- **Consenso obbligatorio** per attività di marketing e profilazione.
  Non ci interessa!
- **Portabilità**: l'interessato può chiedere a chi tratta i dati di inoltrarli a una terza parte in sua vece.
  Non ci interessa!

Responsabile del Trattamento

Fermo restando che il Titolare del Trattamento può essere solo il Legale Rappresentante e tale ruolo non può essere demandato, è possibile individuare un **Responsabile del Trattamento**.

Questo ruolo dovrebbe essere ricoperto dalla persona che più di chiunque altro si occupa del trattamento dei dati e che coordina le attività di trattamento.

La figura del Responsabile è obbligatoria solo nel caso si trattino dati sensibili, quindi per noi è una figura assolutamente opzionale.

Il Responsabile è anche colui o colei a cui fanno capo gli Incaricati al Trattamento.

Incaricati al Trattamento

Con la precedente normativa era obbligatorio identificare gli **Incaricati al Trattamento**, ossia coloro che ricevevano il compito di svolgere le effettive operazioni di trattamento (acquisizione, archiviazione, utilizzo dei dati).

Ogni Incaricato aveva il dovere di firmare una Lettera di Incarico, in cui tutte queste modalità venivano definite.

Né le Lettere di Incarico, né le figure degli Incaricati stessi sono più obbligatorie. Chiunque può essere un Incaricato, quando tratta i dati per conto dell'Associazione. In quel caso deve accertarsi di:

- rendere l'informativa all'interessato, all'atto della raccolta dei dati,
- trattare i dati nel rispetto dell'informativa,
- in seguito alla raccolta, comunicare le modifiche alle modalità di trattamento,
- cancellare i dati qualora non si rivelassero più necessari.

Misure di sicurezza

Le misure di sicurezza impiegate devono essere adeguate e proporzionate all'importanza dei dati protetti.

Tutti gli operatori che operano con i dati devono essere informati sui rischi e le procedure per prevenirli, senza per questo sfociare nella psicosi.

È sempre necessario considerare:

- la sensibilità dei dati,
- l'entità e la numerosità dei dati e
- il formato e la modalità di conservazione.

Per assurdo, 1000 indirizzi e-mail salvati in un singolo file di testo su un computer hanno più valore di 100000 schede d'iscrizione cartacee di altrettanti soci. Infatti, in caso di compromissione dei dati, i 1000 indirizzi possono essere prontamente usati per inviare posta indesiderata, mentre le schede cartacee richiederebbero per ottenere lo stesso risultato di molto più lavoro.

Diverso sarebbe il caso se le schede contenessero dati sensibili, quali religione, appartenenza a minoranze politiche, preferenze sessuali, o simili. Comunque le valutazioni sulla sicurezza vanno fatte caso per caso.

Liceità del trattamento

È lecito trattare i dati se sussiste una di queste condizioni:

- l'interessato ha fornito il consenso,
- è necessario da contratto stipulato in precedenza,
- è obbligatorio in termini legali (es: inserimento dei dati nel libro soci),
- è necessario ai fini della salvaguardia della vita,
- è richiesto per motivi di interesse pubblico o per l'esercizio di pubblici poteri,
- legittimo interesse reciproco (es: fornire i dati all'assicurazione quando ci si associ a una società sportiva).

Limitazione del trattamento

L'interessato ha sempre diritto alla limitazione del trattamento.

Qualora sia indicato chiaramente nell'informativa, tale limitazione limitazione potrebbe anche significare la cessazione del rapporto. (es: se nell'informativa è chiaramente riportato che, ai fini dell'iscrizione, il socio deve essere iscritto alla newsletter, revocare l'uso dell'e-mail comporta una cessazione del rapporto associativo)

Azioni da intraprendere:

È opportuno che l'Associazione si doti di alcuni strumenti organizzativi, anche se non obbligatori. Dimostrare di avere processi ordinati e controllati è la prima difesa contro eventuali tentativi di rivalsa.

Di seguito presento alcune azioni che a mio avviso potrebbe essere opportuno intraprendere. Si noti che non sono un esperto in termini di normativa. Quanto riporto nasce dalla mia comprensione (parziale) di questo particolare regolamento, suffragata dai pareri esperti da me raccolti durante l'incontro del 25 maggio scorso. Quanto scrivo tiene anche conto della mia conoscenza delle attività di trattamento dei dati correntemente in essere all'interno dell'Associazione.

Identificare le attività di trattamento

È opportuno identificare e definire le attività dell'Associazione che consistono in un'afferenza di dati e nel loro trattamento.

Nella pratica può risultare necessario identificare:

1. **attività:** quali dati sono necessari e per quali scopi,
2. **fonti:** da dove vengono recuperati i dati necessari a ciascuna attività,
3. **acquisizione:** modalità di acquisizione dei dati utilizzati.

In pratica si tratta di un processo a ritroso, a partire da un'analisi di quali dati sono **effettivamente necessari**.

Il vantaggio di questo processo è che ci permette di identificare dei flussi di trattamento (dall'atto dell'acquisizione al momento del trattamento).

Conoscere i flussi ci permette di:

- rifinire l’insieme dei dati trattati, al fine di cancellare tutti quelli che non sono effettivamente necessari,
- implementare correttamente nuovi flussi, identificando di volta in volta le nuove attività ed eventuali nuovi dati da acquisire,
- dismettere correttamente i flussi obsoleti, cancellando di volta in volta i dati non più necessari.

Analizzare le nostre attività come flussi di dati personali ci aiuta anche a mantenere costantemente aggiornata l’informativa.

Situazione attuale:

Sono state identificate le attuali attività di trattamento dei dati e la loro descrizione è stata incorporata nell’informativa.

Non sono state ancora formalizzate secondo lo schema proposto.

Prossimi passi:

Redigere un documento ufficiale dove tali flussi siano definiti in modo formale, in termini di:

- dati trattati
- modalità del trattamento
- finalità del trattamento
- ruoli coinvolti (vedi punto seguente)

Identificare i ruoli coinvolti nel trattamento

Per ciascuna delle attività è opportuno identificare dei ruoli astratti coinvolti nel trattamento.

A livello di analisi, è bene che i ruoli non vengano modellati sugli effettivi ruoli istituzionali entro l’Associazione. Per esempio chi raccoglie i dati personali non è il Referente di Zona, ma un ipotetico Acquisitore.

In questo modo è più facile ragionare su quali persone reali appartenenti all’Associazione ricoprono quali ruoli, in quali circostanze.

Per ogni ruolo, è opportuno definire:

- quali attività è chiamato a svolgere,
- quali criticità può incontrare nell’ambito della sicurezza e dell’integrità dei dati,
- quali pratiche deve applicare per ridurre al minimo l’impatto di tali criticità.

In questo modo diventa più facile strutturare per ciascun ruolo un vademecum specifico e presentare a ciascuna persona un vademecum “complessivo” che rappresenti la somma dei propri ruoli.

Questa attività è interamente da svolgere, possibilmente tramite la stesura di un documento ufficiale, come sopra.

Vademecum per gli incaricati

Identificato ciascun ruolo, dovrebbe essere facile redigere un semplice vademecum, scritto con un linguaggio diretto e informale, che descriva in modo completo le attività da svolgere e le modalità richieste ai fini dell'adempimento normativo.

Conviene scrivere anche un minimo vademecum introduttivo per sensibilizzare tutti gli incaricati alle questioni relative al trattamento dei dati. In pratica basterebbe un'estrema sintesi di quanto riportato nella prima parte di questo documento, assieme a un ricapitolo di alcune norme di buon senso relative al rispetto della privacy e alla sicurezza dei dati.

Insieme alle norme per gli incaricati, è opportuno perfezionare gli estratti dell'informativa da presentare agli interessati (generalmente ai nuovi soci).

Questa attività è interamente da svolgere, a valle dell'individuazione dei ruoli.

Sottoscrizione di responsabilità da parte degli incaricati

Prodotta tutta questa documentazione, sarebbe opportuno redigere una sorta di Lettera d'Incarico, che rappresenti una presa di responsabilità dell'incaricato.

Questa a mio avviso non è tanto da intendersi come scarico di responsabilità in caso di errori, che possono ovviamente verificarsi e rientrano possibilmente nell'ambito del Data Breach. Diventa necessario per tutelarsi in caso di reiterata negligenza o condotta maligna da parte dell'incaricato.