CSVnet
LOMBARDIA
confederazione regionale dei
centri di servizio per il volontariato

GDPR 2016/679
ASSOCIAZIONI E ADEGUAMENTI PRIVACY

Realizzato da CSVnet Lombardia
Confederazione regionale dei Centri di Servizio per il Volontariato

1
Inquadramento generale

Il Regolamento UE 2016/679, entrato in vigore il 25 maggio 2018, innova profondamente la gestione dei dati delle persone, obbligando tutte le organizzazioni che operano nell'Unione Europea a rivedere le proprie modalità di lavoro.

Le finalità del Regolamento 679 sono chiare: **tutelare i dati delle persone fisiche, soprattutto quelli "particolari"** per proteggere le persone, non solo dalle "intemperanze" dei call center, ma anche da usi più pericolosi e criminali dei dati personali (il furto di identità, la diffusione incontrollata di dati personali sensibili, le truffe informatiche, i furti informatici).

Quindi è importante per tutti, ma soprattutto per i responsabili delle organizzazioni, per i volontari ed i lavoratori che accedono a dati sensibili delle persone, conoscere bene le nuove regole ed adottare delle misure adeguate di protezione.

1) Il Regolamento 679 **si applica solo per i dati delle persone fisiche, non per quelli delle società e delle organizzazioni che sono di per sé pubblici**.

2) Il Regolamento 679 distingue tra "***dati personali comuni***" e "***dati personali particolari***". I *dati personali comuni* sono quelli che identificano una persona (cognome e nome, luogo e data di nascita, codice fiscale), la sua reperibilità (residenza, n. telefono, e-mail), le fotografie, i video etc. I *dati personali particolari* (nel vecchio Codice Privacy erano i dati "*sensibili*") sono quelli che identificano alcune caratteristiche particolari di una persona, il loro uso è sottoposto a limitazioni e deve essere sempre controllato e protetto. Sono "*particolari*" i seguenti dati: origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, nonché dati genetici e dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute, dati relativi alla vita o all'orientamento sessuale, dati giudiziari.

3) Il Regolamento 679 prevede che **il trattamento[1] dei dati è legittimo se vi è consenso da parte dell'interessato**. Il consenso può essere implicito o esplicito ma, in ogni caso, **deve essere: inequivocabile; libero; specifico; informato; verificabile; revocabile.**

4) Il regolamento specifica **i diritti che le persone hanno e che possono utilizzare** nei confronti di tutti coloro che trattano i loro dati personali. I diritti sono:
   - **diritto all'accesso**, cioè a conoscere come si stanno utilizzando i loro dati;

[1] È trattamento dei dati 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. A titolo di esempio il trattamento dei dati può essere la raccolta tramite un format ad hoc, la registrazione dei dati in un registro specifico, l'organizzazione dei dati secondo un principio o un ordine, la conservazione in un archivio cartaceo od informatico, l'estrazione da un database, la consultazione, l'utilizzo del dato, la comunicazione o messa a disposizione dei dati a soggetti terzi tramite qualunque mezzo, la cancellazione, la distruzione, etc.

- **diritto all'oblio**, ovvero alla rettifica ed alla cancellazione dei dati;
- **diritto alla limitazione del trattamento**;
- **diritto all'opposizione al trattamento**;
- **diritto a proporre un reclamo** al Garante Privacy.

5) Il regolamento specifica che il **Titolare del trattamento è sempre e comunque il legale rappresentate dell'organizzazione**. In caso di organizzazioni particolarmente complesse può delegare ad un responsabile del trattamento dati tale funzione ma non la responsabilità legale.

2
Gli obblighi del titolare

Il titolare del trattamento deve **rendere esplicito e comunicare chiaramente (a mezzo di apposito documentazione chiamata "*informativa*") la finalità del trattamento prima che il trattamento dei dati abbia concreto inizio**, in modo da consentire all'interessato di fornire un consenso informato (che può essere implicito o esplicito a seconda dei casi). La comunicazione va fatta a mezzo di **apposita documentazione** (*informativa*) che deve essere portata a conoscenza dell'interessato e messa a disposizione a fini di ispezione da parte delle autorità di controllo. In assenza della precisazione della finalità, il trattamento è illegittimo.

Il Regolamento 679 prevede che, per utilizzare e trattare i dati comuni, occorre avere un consenso della persona **specificando sempre**:

- **per quale finalità si stanno raccogliendo i suoi dati** (per esempio, per accedere ad un servizio);
- **a chi verranno comunicati i** dati;
- per **quanto tempo verranno conservati ed utilizzati**;
- **chi è il Titolare del Trattamento**, cioè l'organizzazione a cui la persona che ha conferito i dati può rivolgersi per chiedere chiarimenti.
-

Relativamente i ***dati personali particolari***, **la raccolta e l'utilizzo di questi dati è lecito solo se è stato raccolto un chiaro, libero e consapevole consenso scritto della persona**. Anche per i dati particolari occorre dire, in modo comprensibile:

- **perché**, per quale finalità sono raccolti;
- **per quanto tempo si conservano**;
- **a chi vengono eventualmente comunicati**;
- chi è il titolare del trattamento.

Per tutti i dati "particolari", sia cartacei che digitali:

- **il titolare ha l'obbligo di gestirli in modo controllato e di proteggerli, sempre; le persone autorizzate al trattamento hanno l'obbligo della riservatezza e della correttezza**.

Il regolamento prevede un diverso livello di obblighi da adottare a seconda di tipologia, modalità, mole e finalità di trattamento. In base alle proprie caratteristiche, è quindi consigliabile predisporre la seguente documentazione con i relativi requisiti:

- trattamento esclusivo di "dati personali comuni" e non di "dati personali particolari" o "dati personali" di minori;
- trattamento di un numero di "dati personali comuni" inferiore a 1000 unità;
- nessuna profilazione automatica[2] dei "dati personali trattati";

[2] Per ***profilazione*** si intende l'insieme delle attività di raccolta ed elaborazione dei dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento.

- invio a paesi terzi (extra EU) dei “dati personali trattati”;
- redigere ed aggiornare il registro dei trattamenti.

L’organizzazione che raccoglie i dati delle persone, come titolare del trattamento, deve tener conto della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche; ha quindi i seguenti obblighi:

- attivare misure di sicurezza che riducano il rischio di perdita, acceso involontario o furto dei dati;
- individuare e autorizzare le persone autorizzate al trattamento, promuovendone la formazione;
- notificare al Garante, quale Autorità di controllo, ogni violazione dei dati personali di cui si venga a conoscenza, qualora da questa derivino rischi per i diritti e le libertà degli interessati.

3

La documentazione da predisporre e tenere

1. Redigere il **REGISTRO DEI TRAMMENTI DEL TITOLARE**.
2. Sulla base delle informazioni contenute nel Registro dei trattamenti del titolare redigere (o aggiornare) l'**INFORMATIVA**.
3. Se i dati raccolti sono necessari all'invio della newsletter, di posta ordinaria, di contatto telefonico, etc. allora è necessario **elaborare (o aggiornare) un CONSENSO INTEGRATIVO ALL'INFORMATIVA**.
4. Devono essere elaborati (o aggiornati) i **documenti di NOMINA** per gli autorizzati al trattamento unitamente al loro **IMPEGNO ALLA RISERVATEZZA**.

NB: si rimanda all'allegato REGISTRO DEI TRATTAMENTI DEL TITOLARE, all'allegato CONSENSO ED INFORMATIVA e all'allegato NOMINA ED IMPEGNO ALLA RISERVATEZZA per i FACSIMILI e la guida alla compilazione di questi documenti.

4
Le misure di sicurezza da adottare

Tutti i documenti che contengono dati di persone fisiche devono essere protetti. Questo significa che:

- i **documenti cartacei** devono essere raccolti, tenuti e gestiti, in locali tendenzialmente chiusi al pubblico (od ad accesso controllato); se contengono dati particolari (sensibili) devono essere archiviati in armadi con serrature; non devono essere lasciati incustoditi;
- i **documenti digitali** (informatici) devono essere raccolti, tenuti e gestiti su personal computer o desktop, isolati od in rete, protetti con antivirus e firewall; particolare attenzione va posta all'utilizzo della posta elettronica, che rimane lo strumento più attaccabile dai virus informatici; occorre fare molta attenzione all'uso degli smartphone perché spesso sono dei veri archivi mobili (se si scaricano le mail, se si scambiano documenti con Whatsapp, Instagram, Messanger o software simili) e come tali vanno protetti.

Quindi vi sono due condizioni organizzative che devono essere sempre valutate:

- la **situazione della sede reale dell'organizzazione**, che deve essere esclusiva e controllata, con arredi (scrivanie, cassettiere, armadi ecc.) preferibilmente dotati di chiusure con chiavi;
- la **gestione delle apparecchiature informatiche**, qualsiasi sia la loro configurazione (personal portatili o desktop, isolati od in rete) devono essere installati sistemi di protezione (antivirus, firewall ecc.) e periodicamente verificati e mantenuti; una corretta gestione e manutenzione non riguarda solo i computer ma anche le altre apparecchiature elettroniche eventualmente utilizzate, come stampanti, scanner, modem ecc; una soluzione utile è quella di utilizzare archivi in *cloud* (ricordando che il loro grado di protezione dipende dal costo e che, quindi, quelli gratuiti non sono molto protetti);
- **organizzazione di incontri periodici di formazione** (documentati con foglio firme) in cui si ribadiscono ai volontari e agli autorizzati al trattamento dati i principi ed i comportamenti da rispettare per garantire il corretto trattamento;
- dopo aver avuto il consenso al trattamento dei dati, l'organizzazione (e le persone) che le gestiscono devono quindi **garantire la loro protezione**; questo rischia di essere piuttosto difficile se i dati ed i documenti sono sparsi in molti (troppi) archivi.