



ASSOCIAZIONE FAMIGLIE ADOTTIVE PETALI DAL MONDO ONLUS
INFORMATIVA PER LA GESTIONE DEI DATI DELLE PERSONE FISICHE
(Regolamento UE 2016/679)

PETALI DAL MONDO ONLUS
Associazione Famiglie Adottive

Il Regolamento UE 2016/679, entrato in vigore il 25 maggio scorso, 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 sono chiare: fare in modo che i dati delle persone fisiche, in modo particolare quelli "particolari" siano tutelati e protetti. Obiettivo è proteggere le persone, non solo dalle "intemperanze" dei call center, ma anche da usi più pericolosi dei dati personali: il furto di identità, la diffusione incontrollata di dati personali particolari, le truffe informatiche, i furti informatici.

Quindi è importante per tutti, ma soprattutto per coloro che per lavoro accedono a dati particolari delle persone, conoscere bene le nuove regole ed adottare tutti gli accorgimenti di protezione possibile, tenendo presente che i minori e le persone che hanno bisogno dei servizi formativi e per il lavoro, o che si trovano in una situazione di difficoltà, sono da tutelare maggiormente.

Il Regolamento prevede delle sanzioni elevate per le imprese e le organizzazioni che non si mettono in regola.

La prima importante precisazione: il Regolamento si applica **solo per i dati delle persone fisiche**, non per quelli delle società e delle organizzazioni.

Il Regolamento 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), l'IBAN. In ogni caso il Regolamento 679 prevede che, per utilizzare e trattare i dati comuni, occorre avere un consenso sottoscritto dalla persona. Nel modulo per la raccolta del consenso bisogna chiarire:

- per quale finalità si stanno raccogliendo i suoi dati (per esempio, per accedere ad un servizio sanitario, formativo, per il lavoro),
- a chi verranno comunicati e 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.

Il Regolamento 679 individua anche dei **dati personali particolari** (nel vecchio Codice Privacy erano i dati "sensibili"), per i quali è obbligatorio utilizzare ulteriori protezioni:

- è sempre richiesto il consenso **scritto** della persona,
- devono essere tenuti e trattati in modo ancor più riservato rispetto ai dati comuni, in ogni fase del loro utilizzo.

Il Regolamento fa un elenco preciso dei dati particolari (sensibili): essi sono i dati personali che rivelino:

-
- l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici, i dati relativi alla salute, i dati relativi alla vita o all'orientamento sessuale della persona, i dati giudiziari.

Quindi tutti i dati relativi alla salute di una persona sono da considerarsi dati "particolari", da trattare con maggiore cautela e riguardo.

Il Regolamento 679 definisce anche i **diritti** che le persone hanno e che possono utilizzare nei confronti di coloro che trattano i loro dati personali. I diritti sono:

- il diritto all'accesso, cioè a conoscere come si stanno utilizzando i loro dati, alla rettifica ed alla cancellazione (diritto all'oblio), alla limitazione del trattamento, all'opposizione al trattamento, il diritto di proporre un reclamo al Garante Privacy.

Dopo aver avuto il consenso al trattamento dei dati, l'organizzazione, tramite le persone che le gestiscono, **devono garantire la loro protezione**. E ciò rischia di essere piuttosto difficile se i dati ed i documenti sono sparsi in molti (troppi) archivi.

In primo luogo vanno protetti gli archivi cartacei: i documenti devono essere conservati in un luogo chiuso, ad accesso controllato (non aperto al pubblico) e, nel caso di documenti con dati particolari in armadi (od in locali) che si possono chiudere a chiave. I documenti con dati particolari non vanno mai lasciati incustoditi.

Vanno protetti anche gli archivi informatici; meglio se sono salvati su un solo server protetto con password, antivirus e firewall (anti-intrusione). Se sono conservati su più strumenti (personal computer, tablet, smartphone, chiavette USB ecc.) la loro protezione diventa ancora più difficile; ma è sempre necessaria. La protezione degli archivi informatici deve essere garantita dai tecnici, ma resta fondamentale il ruolo degli operatori, che devono sapere sempre adottare i comportamenti più corretti (e prudenti).

Gennaio 2019