25/05/2018:
GDPR n.679/2016
REGOLAMENTO GENERALE per la PROTEZIONE dei DATI

In via di abrogazione: Codice della Privacy (d.lgs.196/2006)

nato dalla Dir. 95/46 CE

AIAV
ASSOCIAZIONE ITALIANA AGENTI DI VIAGGIO

FINALITÀ?

UNICO REGIME DI PROTEZIONE DEI DATI COMUNE A TUTTO IL TERRITORIO UE

Applicabilità diretta

- in tutti gli stati UE
- nei confronti di tutti soggetti che svolgono affari sul suolo europeo, anche se con sede extra UE

Obiettivi

- Aggiungere la Protezione dei dati nel novero dei diritti fondamentali
- Creare un mercato digitale europeo uniforme (libera circolazione dei dati)
- Ricreare un rapporto di fiducia tra tecnologia, impresa e consumatori

Considerando n. 7

È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

Cos'è un «**Dato Personale**»?

Qualsiasi informazione riguardante una persona fisica («interessato») che possa identificarla direttamente o indirettamente:

- nome;
- numero di identificazione;
- dati relativi all'ubicazione;
- identificativo online;
- elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

COME ADEGUARSI?

1° step:
il Titolare determina finalità e mezzi di trattamento

PERCHÈ RACCOGLI DATI?

- Individua base giuridica e finalità del trattamento (consenso, esecuzione di contratto, salvaguardia interessi vitali, obblighi di legge, interesse di un terzo…)

COME ADEGUARSI?

1° step:
il Titolare determina finalità e mezzi di trattamento

COME SI RACCOLGONO I DATI ?

Seguendo i principi di liceità, correttezza e trasparenza;

Per espresse finalità

Adeguati pertinenti e limitati – minimizzazione dei dati

Esatti ed aggiornati

Conservati per un tempo congruo

(Art. 5)

COME ADEGUARSI?

1° step: il Titolare determina finalità e mezzi di trattamento

Il **consenso**: deve

- essere liberamente prestato
- specifico
- informato (identità titolare, finalità, tipo di dati, diritto di revoca, trasferimento dati paesi extra UE)
- indicare univoca di volontà
- essere esplicito (non necessario scritto ma più sicuro)

• Il **consenso** dei minori valido dai 16 anni

Raccomandazioni:

Il consenso dato prima del 25/05/18 è valido solo se ha caratteristiche sopra individuate: se no, va raccolto **nuovamente**

COME ADEGUARSI?

1° step:
il Titolare determina finalità e mezzi di trattamento

Come predisporre l'INFORMATIVA

- elenco TASSATIVO Art.13 -

Tra gli altri:

a) **identità e dati di contatto del titolare del trattamento**

b) i dati di contatto del **responsabile**

c) **finalità trattamento**

d) **intenzione del titolare trattamento di trasferire dati personali a un paese terzo**

e) **periodo di conservazione dei dati**

f) **diritto dell'interessato** di **presentare reclamo**

ATTENZIONE

- il *Registro Attività di Trattamento*: **obbligatorio** per imprese con più 250 dipendenti, ma **utile per tutti** per una gestione più efficace ed ordinata della sicurezza dei dati

COME ADEGUARSI ?
2° step:

Adottare **misure di protezione**

Principio di
RESPONSABILIZZAZIONE
(accountability)

- Adotta le misure di protezione tecniche e organizzative necessarie per assicurare la conformità della raccolta alle norme
- Valuta caso per caso e già in fase di progettazione del trattamento
- Interessa tutti i livelli e le aree dell'azienda

COME ADEGUARSI ?
2° step:

Adottare **misure di protezione**

RENDERE SICURO IL TRATTAMENTO!

attraverso **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**

Es:

- a) pseudonimizzazione e cifratura dei dati personali;
- b) assicurare su base permanente riservatezza, integrità, disponibilità e resilienza di sistemi e servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Come adeguarsi?

3° step
Il Titolare valuta il RISCHIO di VIOLAZIONE

COME ?
- privacy by design & by default -

È fondamentale per la corretta gestione del ciclo di trattamento:

- valutazione preventiva e sistematica della finalità e necessità di trattamento, di tutela dei diritti degli interessati in caso di violazione tenendo conto del contesto
- Con quanta facilità potrebbero essere identificati gli interessati?
- Danni?

Come adeguarsi?
4° step

In caso di VIOLAZIONE dei DATI

Comunicare la violazione all'autorità di controllo - Garante Privacy - **entro 72 ore** dalla conoscenza.

ANCHE agli interessati, se c'è pericolo per loro libertà e diritti .

Al fine di incentivare il vantaggio competitivo delle aziende

Limitazione del titolare

- Principio di minimizzazione della raccolta dei dati

Ampliamento diritti degli interessati

- Diritto all'informazione
- Diritto all'accesso
- Diritto alla rettifica e cancellazione
- Diritto di opposizione
- Diritto alla portabilità dei dati

Bilanciamento interessi di titolare e interessato

- Nella maggior parte dei casi si dovrà ricorrere ad un consenso aggiornato e conforme alla normativa, e dunque inequivocabile, libero, specifico, informato, verificabile e revocabile.
- Pena: quadro **sanzionatorio** severo

Quindi…
cosa devo fare?

- Valutazione del rischio in funzione dell'adeguatezza dei sistemi informatici (ad esempio tipo di dati, sistemi di criptazione, ecc…)
- Individuare le banche dati
- Formazione del titolare e dei dipendenti (*accountability*)
- Organigramma della privacy (titolare, dipendenti, responsabile del trattamento)
- Adottare misure di sicurezza a protezione dei dati e dei sistemi informatici
- Registro delle attività di trattamento (foglio di Excel)
- Predisporre una informativa privacy chiara e trasparente, che risponda ai requisiti di cui agli artt. 13 e 14
- Consenso

Check list

- Ho predisposto i moduli per al raccolta del consenso?
- Ho predisposto la privacy policy?
- Ho individuato i dati «essenziali» per la mia attività?
- Ho organizzato la conservazione dei dati cartacei ed informatici?
- Ho stabilito un tempo?
- Ho fatto formazione per me e per i miei collaboratori?
- I miei strumenti informatici (pc, chiavette usb, memorie esterne) sono protetti da minacce esterne?
- Backup?
- Ho pensato alla sicurezza «fisica» dell'agenzia?

I 4 cantoni

- 1) Valutazione del rischio
- 2) «Privacy Policy» e «Modulo del consenso» da far firmare al cliente
- 3) Sicurezza informatica e fisica dell'adv

Contenuto della privacy policy

Il presente documento contiene informazioni importanti su quanto segue:

- 1. Trattamento dei dati personali
- 2. Dati personali raccolti
- 3. Finalità del trattamento dei dati personali
- 4. Comunicazione dei dati personali
- 5. Tutela della privacy dei minori
- 6. Archiviazione, accessibilità e trasferimento dei dati personali
- 7. Sicurezza e riservatezza dei dati personali
- 8. Diritti di accesso ai dati personali e gestione delle scelte
- 9. Conservazione dei dati
- 10. Politica in materia di cookie e processi analoghi
- 11. Collegamenti, inserzionisti, sponsor e pubblicità
- 12. Titolare del trattamento - contatti della società
- 13. Aggiornamenti della informativa

Contenuto del modulo per la raccolta del consenso

- Letta l'informativa privacy, acconsento al trattamento dei dati personali forniti, per le seguenti finalità:

- esecuzione del contratto (obbligatorio)
- invio di newsletter (facoltativo)
- cessione a terzi (facoltativo/obbligatorio)

FINE

Grazie per l'attenzione!

Avv. Veronica Scaletta – legale.scaletta@aiav.eu

Dott.ssa Federica Benincasa – legale.benincasa@aiav.eu

Il Titolare del Trattamento (Data Controller)

Il Titolare del Trattamento è chi determina, da solo o insieme ad altri, le finalità e gli strumenti del trattamento di dati personali e decide quali categorie di dati personali devono essere registrate ed è responsabile giuridicamente della conformità degli obblighi previsti normativi.

A lui spetta nominare il Responsabile del Trattamento, insieme al quale pone in atto le misure tecniche ed organizzative volte a garantire un livello di sicurezza adeguato al rischio.

Nel settore privato il titolare del trattamento può essere una persona fisica oppure una persona giuridica, mentre nel settore pubblico è rappresentato dall'autorità, ovvero da una persona giuridica.

Nel caso di gruppi di società, la società madre e le controllate sono distinti titolari del trattamento, avendo una personalità giuridica distinta. In questo caso il trasferimento dei dati tra le società del gruppo deve essere autorizzata dagli interessati.

Possono esistere più titolari del trattamento che decidono congiuntamente di trattare i dati per una finalità comune, cosa che impone ai contitolari di definire specificamente il rispettivo ambito di responsabilità e i compiti.

Il Responsabile del Trattamento (Data Processor)

Il responsabile del trattamento è "*la persona fisica o giuridica […] che tratta dati personali per conto del titolare […]*".

In pratica è un soggetto al quale vengono delegati dei trattamenti da parte del titolare: nel momento in cui viene affidato un servizio all'esterno, se il soggetto al quale viene affidato il servizio opera "*per conto*" del titolare, siamo in presenza di un responsabile.

Il responsabile del trattamento è completamente assoggettato al potere direzionale del titolare dal quale non solo deve ricevere istruzioni scritte, ma deve anche rispettarle scrupolosamente. Inoltre è compito suo (o del titolare) tenere il registro dei trattamenti.

In caso di mandato ricevuto dal Titolare del trattamento, spetta al Responsabile del trattamento la nomina del responsabile per la protezione dei dati (DPO).

Il Responsabile della Protezione dei Dati (DPO)

Tra le garanzie che il responsabile del trattamento dovrà offrire al titolare c'è anche la nomina del DPO che ha il compito di facilitare l'applicazione della normativa (è anche stato definito "*facilitatore*").

In base al GDPR, non solo i titolari, ma anche i responsabili del trattamento sono tenuti a nominare un DPO e la sua nomina è obbligatoria per tutte le autorità pubbliche e per altri soggetti che trattino su larga scala categorie particolari di dati personali e per aziende con più di 250 dipendenti.

Il DPO «*è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*».

Anche se non vengono specificate le qualità professionali da prendere in considerazione nella nomina di un DPO, è utile ci sia la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento.

È essenziale che al DPO siano garantite autonomia e indipendenza e non deve assolutamente ricevere istruzioni dal titolare.

Anche se la tenuta del registro dei trattamenti non rientra tra le sue mansioni, nulla vieta che il titolare o il responsabile possano affidare a lui questo compito.