PRIVACY

Gestione e contitolarità dei dati personali nel quadro della “compliance” aziendale

Le figure del titolare e del responsabile del trattamento e del responsabile della protezione dei dati

di Damiano Marinelli , Chiara Rossi | 20 FEBBRAIO 2018

Il 25 maggio 2017 è entrato in vigore il Regolamento europeo 27 aprile 2016, n. 2016/679/UE, sulla protezione dei dati personali (cd. GDPR), approvato dal Parlamento europeo in data 14 aprile 2016. Tale regolamento, di portata generale e obbligatorio in tutti i suoi elementi, sarà direttamente applicabile negli Stati membri dell'Unione europea a decorrere dal 25 maggio 2018; da quella data cesserà difatti di avere efficacia il D.Lgs. 30 giugno 2003, n. 196 (codice *privacy*).

SOMMARIO:

Introduzione

Il Regolamento europeo 27 aprile 2016, n. 2016/679/UE, in materia di protezione dei dati personali, comporta numerose novità anche per le **aziende**, sia pubbliche che private, le quali dovranno necessariamente adeguarsi al dettato europeo, che ha previsto un severo **inasprimento delle sanzioni** amministrative. Tra le novità più importanti si può osservare un complesso sistema di **contitolarità del trattamento dei dati personali**, all'interno del quale intervengono **diverse figure**; tra queste va senz'altro annoverata quella del **DPO - Responsabile della protezione dei dati**.

Andiamo ora ad esaminare in modo sintetico i singoli soggetti, rispettando l'ordine previsto dalla normativa.

Il titolare del trattamento

In base a quanto previsto dall’art. 25 del Reg. UE, il titolare del trattamento mette in atto tutte le **misure tecniche e organizzative** adeguate al fine di **attuare** efficacemente la **protezione dei dati**. Tra le più importanti **misure di sicurezza** messe in atto vanno senz'altro menzionate:

- la pseudonimizzazione, la minimizzazione, la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati, in caso di incidente fisico o tecnico;

- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative, al fine di garantire la sicurezza del trattamento.

Nomina del responsabile del trattamento

Il titolare nomina a sua volta un responsabile del trattamento, attribuendogli **specifici compiti**. Il "responsabile del trattamento dei dati personali" è la "figura" di vertice cui competono le **decisioni** in ordine alle finalità, alle **modalità del trattamento** di dati personali e agli **strumenti utilizzati**, ivi compreso il profilo della **sicurezza dei dati**. il responsabile del trattamento (art. 4 , n. 8) è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*". La **nomina** avviene attraverso la stipula di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve tassativamente disciplinare almeno tutte le materie riportate al par. 3 dell'art. 28, al fine di dare dimostrazione che il responsabile fornisca "garanzie sufficienti".

Attenzione

L e **garanzie richieste** riguardano in particolare natura, durata e finalità del trattamento o dei trattamenti assegnati. Così come deve essere garantito che le categorie di dati oggetto di trattamento e le misure tecniche e organizzative siano adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento.

Con la stipula di un contratto, il **titolare delega** al responsabile la concreta gestione del trattamento, affidandogli uno o più compiti specifici oppure una serie di compiti dettagliati in generale. Il responsabile a sua volta può nominare **responsabili di secondo livello**, a meno che non sia vietato dalle istruzioni del titolare. E' comunque il responsabile principale a rispondere dell'operato degli altri da lui nominati, di fronte al titolare del trattamento.

Attenzione

Nel caso in cui il responsabile del trattamento ecceda i limiti di utilizzo dei dati fissati dal titolare, il responsabile diventa titolare della **gestione illecita** dei dati e ne risponde come tale, insieme all'effettivo titolare (in sostanza è come se diventassero contitolari).

Contitolarità della responsabilità

La normativa prevede la possibilità di **gestire congiuntamente la titolarità del trattamento dei dati** ed essere quindi contitolari della stessa responsabilità.

L'art. 26 impone ai titolari di **definire specificamente** (con un atto giuridicamente valido ai sensi del diritto nazionale) il **rispettivo ambito di responsabilità e i compiti** con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente.

Obbligo di tenere un registro delle attività di trattamento

Il regolamento *privacy* europeo obbliga alla redazione di un registro dei trattamenti che illustri in modo molto dettagliato:

- la tipologia dei dati trattati;
- chi vi ha accesso;

- come vengono utilizzati;
- per quanto tempo vengono conservati.

Evidentemente, questo registro deve rappresentare una fotografia fedele di quanto accade nell'azienda. Nel caso in cui il titolare del trattamento abbia **delegato alcune attività ad un responsabile**, lo stesso ha altrettanto l'obbligo di tenere un registro relativo a tutte le attività svolte. I registri sono tenuti in **forma scritta** e anche in **formato elettronico** e, su richiesta, devono essere messi **a disposizione dell'autorità di controllo**.

Attenzione

In caso di **accesso abusivo** a dati personali o **perdita** degli stessi (il cosiddetto *data breach*), è necessaria in alcuni casi una notifica al Garante e perfino ai singoli individui i cui dati sono stati oggetto del *data breach* (con ovvia problematica rispetto alla propria **affidabilità verso il consumatore/utente**).

Il responsabile della protezione dei dati - "Data protection officer" (o DPO)

La normativa europea richiede alle aziende di adottare un sistema di *policy* e misure organizzative e tecniche che consentano di avere un **controllo continuo** sulla conformità dell'azienda con la normativa *privacy* e che quindi siano sempre "*work in progress*". Questa attività è supportata dalla nomina del *data protection officer* (o DPO), che è una delle grandi novità del regolamento; tale figura, storicamente già presente in alcune legislazioni europee, è un professionista che deve avere un **ruolo aziendale** (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di *risk management* e di analisi dei processi. La sua **responsabilità principale** è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda, affinché questi siano trattati nel rispetto delle normative *privacy* europee e nazionali.

La figura del DPO è designata dal titolare e dal responsabile del trattamento ed è soggetta ad un **rinnovo periodico**. Potrà essere sia un dipendente dell'azienda, che un collaboratore esterno con regolare contratto. Il soggetto scelto dovrà avere caratteristiche e *skill* tali che permettano lo svolgimento delle sue funzioni in maniera ottimale. Un errore nella scelta (magari per esigenze economiche) implicherebbe una nuova responsabilità del titolare.

Quando è prevista la presenza del DPO?

In base all'art. 37 , viene designato un responsabile della protezione dei dati ogniqualvolta:

a. il **trattamento è effettuato da un'autorità pubblica** o da un organismo pubblico, eccettuate le autorità giurisdizionali, quando esercitano le loro funzioni giurisdizionali;
b. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**;
c. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di **categorie particolari di dati personali** di cui all'art. 9 (dati particolari sensibili) o di dati relativi a **condanne penali e a reati** di cui all'art. 10.

L'art. 9 del regolamento, al comma, 1 definisce quelle che sono le categorie particolari di dati personali (ex dati sensibili) ed in specie i dati personali che: "*rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*".

I principali compiti del DPO

I principali compiti del *data protection officer* sono:

a. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b. sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla

protezione dei dati, nonché delle politiche del titolare del trattamento o del responsabile del trattamento *in materia di protezione dei dati personali*, compresi l'***attribuzione delle responsabilità***, *la* ***sensibilizzazione*** *e la* ***formazione del personale*** che partecipa ai trattamenti e alle connesse attività di controllo;

c. ***fornire***, se richiesto, *un* ***parere in merito alla valutazione d'impatto*** sulla protezione dei dati e ***sorvegliarne lo svolgimento*** ai sensi dell'art. 35;
d. cooperare con l'autorità di controllo;
e. ***fungere da punto di contatto per l'autorità di controllo*** per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, **consultazioni** relativamente a qualunque altra questione.

Attenzione

Si deve sottolineare come in futuro la conformità con la normativa *privacy* e la certificazione della stessa diventerà sicuramente un **pre-requisito** per potere stipulare contratti con banche, assicurazioni, o partecipare ad appalti con soggetti pubblici.

Considerazioni conclusive

In sintesi, rispetto alla normativa precedente i **cambiamenti più significativi** sono:

- **sanzioni** applicabili in caso di violazioni, **aumentate fino a 20 milioni di euro o al 4 per cento del fatturato** mondiale della società che commette la violazione (in precedenza una delle più alte sanzioni determinate nell'UE per la violazione della normativa *privacy* è stata di un milione). Inoltre, ed in conseguenza diretta a queste sanzioni amministrative si pensi alle eventuali **azioni di responsabilità** da parte degli azionisti nei confronti degli amministratori che non abbiano adottato le necessarie misure o alle possibili azioni da parte dei clienti i cui dati siano stati violati, oltre alle **sanzioni di carattere penale**;
- il regolamento *privacy* europeo vincola alla compilazione di un **registro dei trattamenti** che "disegni" in modo molto dettagliato:
  - la tipologia dei dati considerati;
  - chi vi ha accesso;
  - come vengono utilizzati;
  - per quanto tempo vengono conservati.

E spesso la **perdita o accesso abusivo** (*data breach*) va comunicata agli utenti (si pensi alla perdita accidentale di una chiavetta USB contenente dei dati ...);

- non è più solo necessario un controllo atti/documentazione formale, ma un **controllo effettivo e *working progress*** (come per il modello 231), secondo il concetto di ***privacy by design*** che impegna a provare di avere adottato misure determinati per tutelare la *privacy* dalla ideazione di qualsiasi servizio che tratti dati personali;

Esempio

Anche se non formalmente prescritto, sarà fondamentale la **formazione** (e la certificazione della stessa) per **dipendenti dell'azienda**.

- nasce un vero e proprio **diritto alla portabilità dei dati**, che consente agli utenti (e anche dipendenti o qualunque persona i cui dati sono trattati da un terzo) di potere "trasferire" gli stessi dati.

Riferimenti normativi:

- Regolamento europeo 27 aprile 2016, n. 2016/679/UE, artt. 24 - 31 e 37 - 39 .

Argomenti trattati

PRIVACY TRATTAMENTO DEI DATI PERSONALI TITOLARE DEL TRATTAMENTO DEI DATI RESPONSABILE DEL TRATTAMENTO DEI DATI RESPONSABILE DELLA PROTEZIONE DEI DATI COMPLIANCE AZIENDALE