STUDIO TENTORIO

Commercialisti - Revisori legali dei conti

Dott. Franco Tentorio
Dott. Luigi Grumelli Pedrocca
Dott. Claudio Ravasio
Dott. Cristiano Rossetti
Dott. Massimo Marchetti
Dott. Ottorino Tentorio
Dott.ssa Francesca Tentorio
Dott.ssa Alessandra Paganessi

Bergamo, 6 aprile 2018

Spettabili
DITTE CLIENTI
Loro indirizzi

Circolare n. 2/2018

PRIVACY

Regolamento UE 2016/679- General Data Protection Regulation (GDPR)

***

Entro il 25 maggio 2018, tutti i titolari che trattano dati relativi a persone fisiche dovranno adeguarsi a quanto previsto dal Regolamento in oggetto

Il nuovo impianto normativo basa ogni trattamento di dati sui principi di: liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza; riprende e aggiorna il Codice privacy.

In generale:
- vengono introdotti nuovi adempimenti a carico del titolare del trattamento, che comportano una maggior responsabilizzazione (accountability);
- viene resa più dettagliata l'analisi dei rischi, e si evidenzia l'obbligo di pianificazione di misure di sicurezza e di un sistema organizzativo che preveda e consenta il trattamento dei dati nel rispetto di tutti i principi fondanti del GDPR, con verifica periodica;
- vengono ampliati i diritti dell'interessato;
- vengono inasprite le sanzioni.

Più dettagliatamente il GDPR:

1) **DISTINGUE TRA DATI COMUNI E DATI PARTICOLARI** (ex sensibili e giudiziari)
2) **INDICA LE FIGURE INTERESSATE** al trattamento dei dati:

a) titolare del trattamento: come già previsto dal Codice privacy è la persona fisica/ giuridica cui competono le decisioni relative alla gestione dei dati, e conseguentemente le responsabilità;
b) responsabile del trattamento: è la persona fisica/giuridica, preposta dal titolare al trattamento dei dati personali; può essere una persona interna alla struttura, o una società/studio esterno.
Il Regolamento prescrive che il titolare e il responsabile devono redigere un "un atto giuridico", principalmente un contratto in cui esplicitare obblighi e diritti del responsabile, finalità del trattamento, durata, modalità, compiti e responsabilità.
c) persone autorizzate al trattamento dei dati (incaricati del trattamento)**:** persone che trattano i dati, nominate in forma scritta dal titolare o dal responsabile.
d) data protection officer (DPO): è un consulente in possesso di specifiche competenze. E' nominato ove siano presenti trattamenti su larga scala, profilazione o marketing. La nomina deve essere comunicata al Garante.
e) interessato: soggetto i cui dati vengono trattati.

3) RIBADISCE ED AMPLIA GLI OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

Informativa: obbligatoria in caso di trattamento dati di persone fisiche. Può essere fornita in varie forme, anche oralmente. L'onere della prova è a carico di chi la fornisce.
Si distingue tra informativa sui dati raccolti presso l'interessato e dati non forniti direttamente dall'interessato, sia per il contenuto che per la tempistica.

Consenso : obbligatorio per dati particolari; è opportuna la forma scritta (per onere della prova). Deve essere lecito, libero, informato, esplicito, cioè chiaro e ben distinto da altra documentazione. L'interessato può revocarlo in qualsiasi momento.

Data breaches (violazione di dati): il titolare, in caso di violazione dei dati e di accesso abusivo, ha l'obbligo di avvisare l'Autorità di controllo e in casi gravi anche l'interessato entro 72 ore dall'evento.

Privacy by default (minimizzazione dei dati): il titolare deve utilizzare sistemi e applicativi di regola tarati sull'uso minimo e indispensabile dei dati personali per le finalità per le quali sono stati acquisiti.

Privacy by design (pianificazione): il titolare ha l'obbligo "preventivo" di valutare i rischi e pianificare le misure (non più minime ma "adeguate") per assicurare correttezza, integrità, riservatezza e sicurezza dei dati, nonché l'effettiva cancellazione quando richiesto.

Accountability (responsabilità): in caso di controversie il titolare dovrà dimostrare di aver attuato le misure "adeguate" per ridurre al minimo i rischi di perdita dei dati o la loro violazione.

Registro dei trattamenti: non è obbligatorio per aziende con meno di 250 dipendenti, tranne che il titolare, pur in modo occasionale, tratti dati "particolari", cioè ad es. dati sensibili, biometrici, genetici e/ giudiziari.

Valutazione d'impatto sulla privacy (DPIA) : riprende in modo più dettagliato ed esaustivo il Documento programmatico previsto dal Codice privacy.
E' obbligatoria se una determinata tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche". Tra tali tipologie rientrano anche i dati particolari (sensibili e giudiziari); l'obbligo riguarda soprattutto trattamenti su larga scala.
Formazione: è obbligatoria la formazione delle persone che trattano i dati.

4) AMPLIA I DIRITTI DELL'INTERESSATO

Diritto alla portabilità: all'interessato è riconosciuto il diritto di ottenere la restituzione dei propri dati personali trasmessi ad un titolare o a un servizio on line e trasmetterli ad altri (social network, fornitori di servizi internet..)

Diritto all'oblio: l'interessato può ottenere, in particolari circostanze, la cancellazione dei propri dati

Trasferimento di dati all'estero: può avvenire solo in presenza di determinate condizioni, ad es. con il consenso dell'interessato o se necessario all'esecuzione di un contratto. Deve essere chiaramente indicato nell'informativa.

***

SANZIONI: Per violazione dell'obbligo di informativa la sanzione va da 6.000 a 36.000 Euro.
Si prevedono per i casi molto gravi sanzioni fino ad un massimo di 20 milioni di Euro o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

***

VISTA LA COMPLESSITÀ DELLA NORMATIVA E L'ENTITÀ DELLE SANZIONI SI CONSIGLIA DI ATTIVARSI PRESSO IL PROPRIO "CONSULENTE SULLA PRIVACY".
IL NOSTRO STUDIO RESTA A DISPOSIZIONE PER CHIARIMENTI DI BASE.

Studio Tentorio