Studio Associato
Tolone dott. Clelia commercialista
Giovanni Masciosci consulente del lavoro

Sulmona 17 maggio 2018

Circolare n. 03/2018

Spett.li clienti
Loro sede

Oggetto: Nuovo Regolamento Privacy

Gentile cliente

a partire dal prossimo 25 maggio **2018** entrerà pienamente in vigore in tutti i Paesi dell'Unione Europea il nuovo Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali il **GDPR** (*General Data Protection Regulation*).

Al fine di aiutarvi nell'applicazione di questo nuovo metodo di lavoro, vi alleghiamo una serie di **FAQ (quesiti)** che vi aiutano nella comprensione delle problematiche connesse.

Inoltre allegati alla presente circolare troverete i seguenti documenti:

1) Una check list che vi aiuterà nel fare la valutazione dei rischi per la privacy della vostra azienda o attività;
2) Un fac-simile di Informativa da farvi firmare da tutti i vostri clienti e dipendenti ogni volta che vi forniscono dati;
3) Un fac-simile di dichiarazione di consenso da far firmare ai vostri clienti e dipendenti ogni volta che vi forniscono dati;

Le indicazioni contenute in questa circolare, hanno valore indicativo, limitandosi a tracciare le regole basilari comuni previste nel Regolamento comunitario, che come tale è immediatamente e direttamente applicabile nonché imperativo per gli Stati membri ed i singoli cittadini.

Si Resta a disposizione per ulteriori chiarimenti e con l'occasione si porgono distinti saluti.

Tolone Clelia – Masciosci Giovanni

FAQ

Che cos'è il GDPR?

Per "**GDPR**" ("*General Data Protection Regulation*") si intende il nuovo Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali. La nuova normativa entrerà pienamente in vigore in tutti i Paesi dell'Unione Europea il prossimo **25 maggio 2018.**

Il GDPR introduce importantissime novità per cittadini e imprese, con l'obiettivo dichiarato di elevare il livello di protezione dei dati, rafforzare la fiducia dei cittadini e sostenere la crescita dell'economia digitale.

Come faccio a sapere se il GDPR si applica alla mia attività?

Se sei un'azienda o uno studio professionale che tratta dati personali in Italia o in un altro Paese dell'Unione Europea, sei tenuto ad adeguarti al GDPR. Il GDPR si applica anche a imprese ed enti che hanno sede al di fuori dell'Unione Europea, ad esempio se vendono beni o servizi, anche via internet, all'interno dell'Unione Europea.

Ma che cos'è un dato personale?

In pratica, un dato personale è qualunque informazione riconducibile ad un individuo. Ad esempio, sono dati personali il nome e cognome di una persona e tutti i suoi dati anagrafici, l'indirizzo e-mail, il numero di telefono, ma anche una fotografia, i suoi dati biometrici (es. l'impronta digitale o le caratteristiche della sua firma autografa), il suono della sua voce, le sue abitudini alimentari. Alcune categorie di dati (come quelli relativi ai dati genetici, allo stato di salute, all'orientamento sessuale o all'apparenza a partiti e sindacati) sono considerati sensibili e richiedono misure aggiuntive di protezione in base alla normativa.

Quali sono le mie responsabilità come azienda o studio e cosa rischio?

Ai sensi del GDPR, dovrai adottare tutte le misure di protezione dei dati previste dalla normativa. Ecco alcuni esempi di quello che dovrai fare per adeguarti al GDPR:

- informa in modo chiaro, semplice e non "legalese" i tuoi clienti, dipendenti e gli altri interessati di come tratti i loro dati: dì loro chi sei quando richiedi dei dati, perché li stai trattando, per quanto tempo verranno conservati e a chi devono essere comunicati;
- chiedi in modo esplicito il consenso delle persone di cui raccogli i dati; in caso di minori, verifica il limite di età per chiedere il consenso dei genitori;
- assicurati di poter rispondere alle richieste degli interessati: il GDPR attribuisce a tutte le persone il diritto di sapere chi e perché tratta i loro dati, di modificarli, di cancellarli, di opporsi al marketing diretto e alla profilazione, oltre che il diritto di trasferire i propri dati ad un'altra azienda (i.e. portabilità);
- in caso di violazioni di dati o *data breach* – ad esempio, in caso di divulgazione non autorizzata di dati a causa di un problema di sicurezza – dovrai darne comunicazione entro 72 ore all'Autorità di controllo;
- nel caso in cui tu intenda affidare operazioni di trattamento a fornitori o altri soggetti esterni, dovrai assicurarti di ricorrere solamente a responsabili del trattamento che presentino sufficienti garanzie in merito alla conformità al Regolamento e alla tutela dei diritti degli interessati

Il nuovo Regolamento prevede rilevanti sanzioni in caso di violazione, che comprendono multe fino a 20 milioni di Euro o – nel caso di imprese – fino al 4% del fatturato globale dell'esercizio precedente, se superiore.

Cosa devo fare per adeguarmi e da dove cominciare?

La nuova normativa richiede di adottare una serie di misure per proteggere in modo adeguato i dati delle persone con cui la tua azienda o il tuo studio si trova ad operare, ad esempio i dati dei tuoi dipendenti e dei tuoi clienti.

_____

La prima cosa da fare, quindi, è **prendere consapevolezza**:

- Informati (ad esempio qui http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali, http://ec.europa.eu/justice/smedataprotect/index_it.htm e qui https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_it) e valuta quali tra le novità introdotte dal nuovo Regolamento sono applicabili alla tua attività.
- attivati per capire quali dati tratta la tua azienda o il tuo studio, a chi appartengono, per quali finalità li utilizzi, a quali rischi sono esposti e a chi vengono comunicati;
- documenta i trattamenti di dati che hai individuato: il GDPR richiede di tenere (anche in formato elettronico) un Registro aggiornato dei dati personali che gestisci. Il Registro dei trattamenti potrebbe non essere necessario in alcuni casi specifici. Tuttavia, anche in questi casi è raccomandato dal Garante per la Protezione dei dati personali in quanto rappresenta uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte dell'Autorità di controllo, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti svolti ed è uno strumento indispensabile per ogni valutazione e analisi del rischio.

Cosa si intende per "trattamento" di dati personali? Quali trattamenti esegue tipicamente un'azienda o uno studio professionale?

Per "trattamento" si intende qualunque tipo di operazione che viene svolta su dati personali. Ad esempio, raccogliere dei dati creando un archivio o una banca dati, creare copie dei dati, accedere ai dati in lettura o modifica, comunicare i dati a terzi e trasmetterli via internet o con altre modalità sono tutte operazioni di trattamento soggette al GDPR.

I trattamenti sono normalmente descritti – ad esempio ai fini della compilazione del Registro dei trattamenti – attraverso il riferimento a processi o banche dati aziendali.

Ecco alcuni esempi di banche dati e attività la cui gestione rappresenta tipicamente un'operazione di trattamento da parte di studi professionali e aziende:

- anagrafiche clienti
- anagrafiche dipendenti
- anagrafiche fornitori
- videosorveglianza
- campagne commerciali e di marketing
- gestione di un sito web