

Torino, 11 maggio 2018

Ai Sigg. Clienti  
Loro indirizzi mail

## CIRCOLARE N. 2/2018

### PRIVACY

#### **NUOVA NORMATIVA PRIVACY**

Il prossimo 25 maggio entrerà in vigore **il nuovo regolamento privacy UE** (GDPR) n. 679/2016, che sostituirà il vecchio codice della privacy (D.Lgs. 196/2003), che ci interesserà sia come soggetti attivi che passivi.

L'obbligo interessa aziende, professionisti, strutture mediche e in generale tutti coloro che utilizzano dati personali per lo svolgimento delle proprie mansioni.

E' doveroso precisare che è fondamentale essere in regola già a partire dal 25 maggio per evitare le pesanti sanzioni previste.

Il nuovo regolamento pone una particolare attenzione alla **conservazione dei dati digitali**, allo scopo di ridurre il rischio (eliminarlo è impossibile) per:

- Perdita di dati accidentale (mal funzionamento e obsolescenza dei dispositivi, cali di tensione, ecc.);
- Perdita di dati per catastrofi naturali (alluvioni, terremoti, ecc.);
- Sottrazione di dati (furto, hackeraggio e attacchi informatici, terrorismo).

I dati interessati sono quelli delle **persone fisiche**. Nulla è previsto per i dati di società, enti, associazioni.

Sostanzialmente cambia l'approccio a tutto il sistema. La tutela della vita privata degli individui deve essere attuata a monte, come **impostazione predefinita**, e non per semplice adeguamento di esigenze operative di aziende e professionisti.

#### **COME ADEGUARSI**

La materia è veramente complessa, di seguito si riassumono solo gli aspetti principali.

1. Individuazione e nomina del responsabile (interno o esterno)
2. Individuazione dei dispositivi utilizzati (PC, tablet, telefoni, stampanti wi-fi, chiavette usb, servizi clouds, ecc)
3. Analisi dei rischi per ciascuno dei dispositivi utilizzati, connessi a ogni genere di situazione o minaccia.
4. Analisi e messa in pratica di comportamenti atti a ridurre i rischi individuati
5. Sensibilizzare e formare le persone coinvolte nei processi, quali i dipendenti e i collaboratori
6. Individuazione e raccolta documentazione se nei processi sono presenti terze parti, per esempio se si utilizzano servizi di clouds

7. Valutare l'opportunità di crittografare i dati conservati
8. Valutare l'opportunità di codificare i nomi dei file conservati
9. Istituzione di un registro dei trattamenti dove riportare tutte le attività svolte. Il registro è obbligatorio solo per le aziende con oltre 250 dipendenti, ma **se ne consiglia sempre l'istituzione in quanto è l'unico mezzo per dimostrare ciò che stato attuato.**
10. Stesura della documentazione a supporto, sempre completa e aggiornata.
11. Invio e richiesta consenso delle informative a clienti, fornitori e ogni altro soggetto interessato. A differenza della precedente versione, ora occorrerà indicare sempre le finalità della conservazione in maniera chiara e specifica, le modalità di conservazione e le modalità di accesso e verifica da parte degli interessati. Se i dati conservati sono recuperati da terzi (camera commercio, inps, catasto ecc.) occorrerà predisporre un'informativa specifica. Altre tipologie di informative sono previste per chi ha un sito WEB, o utilizza una mailing list, e per i lavoratori dipendenti.
12. I dati raccolti devono poter essere eliminati in maniera definitiva su semplice richiesta dell'interessato

Naturalmente tutto dipende anche dalle finalità di conservazione: un medico e un dentista avranno un onere maggiormente gravoso rispetto a chi detiene dati ai soli fini contabili.

\*\*\*\*\*

Lo Studio è disponibile per ogni ulteriore informazione, nonché a fornire l'assistenza per l'adeguamento al nuovo regolamento.