IUSGATE
Avvocati per l'imprenditore

Conformità privacy in azienda: mappatura, valutazione e regolarizzazione della rete fornitori sono attività fondamentali

Mercredi 3 février 2021

Con un recente provvedimento, **il Garante privacy italiano ha sanzionato, per la somma di 40.000,00 euro** , un fornitore di servizi di prenotazione tramite app (sistema utilizzato da Comuni, pubbliche amministrazioni, strutture sanitarie, professionisti e altri soggetti pubblici e privati) **per diversi profili di illegittimità** riguardanti il trattamento dei dati personali degli utenti.

Senza perdersi nella fitta istruttoria condotta dall'Autorità (che approfondiremo in un contributo dedicato sulla rubrica "Il dato è tratto" della rivista online www.filodiritto.com), **i messaggi pratici e operativi che riteniamo utile estrarre dal provvedimento e comunicare a aziende, imprese e professionisti per evitare cattive prassi e profili sanzionatori**, sono i seguenti:

- **è fondamentale mappare e qualificare – sul piano privacy – la rete di fornitori di servizi** di cui si avvale l'azienda titolare del trattamento;
- tutti i fornitori che, all'esito della mappatura/qualifica, rientrano nella categoria di "**responsabili del trattamento**" (articolo 28 GDPR), **devono sottoscrivere (con il titolare) specifico accordo per disciplinare i trattamenti di dati personali** che derivano dal contratto di servizi e **circoscrivere le reciproche responsabilità**;
- nella maggior parte dei casi, **qualora un contratto di servizi informatici preveda l'attività di assistenza e manutenzione tecnica** (anche da remoto) effettuata sui sistemi informatici dell'azienda titolare, **il fornitore dovrà essere qualificato quale responsabile del trattamento** e, pertanto, **dovrà essere sottoscritto il relativo accordo**;
- tutte le volte che **sono trattati dati relativi alla salute, è necessaria un'indagine specifica volta a individuare l'idoneo presupposto di legittimità** per tale trattamento e le relative **misure di protezione**;
- **è fondamentale**, nell'ambito della gestione dei dati personali trattati per qualsiasi finalità, **fissare e prevedere dei validi criteri di conservazione dei dati personali**, evitando in ogni modo che possa riscontrarsi **la prassi errata (e sanzionabile) della "conservazione indefinita"**.

In sostanza, sempre più, **le indagini del Garante non si limitano ai "classici" inadempimenti** riguardanti, tra le altre, violazioni come l'informativa mancante o inesatta o l'assenza di consenso, **ma si estendono anche alla rete di fornitori dell'azienda e seguono l'effettivo flusso di dati personali**, dall'origine alla loro destinazione.

Ne discende **la fondamentale esigenza di organizzare la privacy aziendale strategicamente, fissando percorsi di miglioramento continuo e adottando un "sistema di gestione" dinamico e aggiornato** , in grado di superare la cattiva – e rischiosa – prassi di archiviare e dimenticarsi i documenti privacy in un file o in un archivio fisico.