GDPR in vigore dal 25 maggio: cosa cambia per le aziende del turismo

Da venerdì 25 maggio entra in vigore ufficialmente il nuovo regolamento europeo per la privacy, noto alle cronache con l'acronimo GDPR, General Data Protection Regulation, come da direttiva europea recepita dall'Italia nel 2016 per dare due anni di tempo alle aziende per adeguarsi.
A febbraio 2016 però il 70% delle aziende non era a norma e gli ultimi mesi sono stati una corsa contro il tempo per adeguarsi alle nuove normative.
Il nuovo regolamento, disciplina solo il **trattamento dei dati personali delle persone fisiche** e si applica ai dati dei residenti nell'Unione Europea. Vale per tutti i tipi di dati personali: nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP. Inoltre, a differenza dell'attuale direttiva, il regolamento si applica anche a imprese ed enti, organizzazioni in generale, con sede legale fuori dall'UE che trattano dati personali di residenti nell'Unione Europea.
La prima cosa che si evince è innanziutto che le aziende che trattano dati di altre aziende non devono preoccuparsi di questo regolamento, anche se ci sono interpretazioni diverse quando l'azienda in questione è un libero professionista o una ditta individuale.
Per le aziende che trattano dati di persone fisiche, ad esempio agenzie viaggi e alberghi, ci saranno diversi nuovi obblighi. Tra questi ci sono innanzitutto **disclaimer informativi ampliati** che devono includere il tempo di mantenimento dei dati personali e in cui occorre fornire i contatti di chi controlla i dati e del funzionario preposto alla protezione dei dati, una nuova figura introdotta dalla legge e nota come DPO, Data protection officer.
È stato inoltre introdotto il **diritto di contestazione delle decisioni automatizzate**, compresa la profilazione. I cittadini hanno ora il diritto di contestare e contrastare decisioni che hanno impatto su di loro e che sono state realizzate unicamente in base ai risultati di un algoritmo.
Tale diritto, fatta eccezione per dati personali intesi ad identificare in modo univoco una persona fisica, non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento,
- si basi sul consenso esplicito dell'interessato.

  Secondo il GDPR un **valido consenso** deve essere esplicitamente dato per la raccolta dei dati e per i propositi per i quali sono usati. I controllori dei dati devono essere in grado di provare il consenso ("opt-in") e il consenso può essere ritirato o modificato con l'introduzione di limitazioni nel trattamento.

  La **sicurezza dei dati** raccolti deve essere garantita dal titolare del trattamento e dal responsabile del trattamento chiamati a mettere in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio, ad esempio la criptazione degli hardware su cui sono conservati i dati.

  Il titolare del trattamento dei dati avrà poi l'obbligo legale di **rendere note le fughe di dati** all'autorità nazionale, presso cui è stato istituito il Registro dei trattamenti dei dati personali, e di comunicarle entro 72 ore da quando ne è venuto a conoscenza. I resoconti delle fughe debbono essere riferite all'autorità sovrintendente non appena se ne viene a conoscenza e comunque entro 72 ore. In alcune situazioni le persone di cui sono stati sottratti i dati dovranno essere direttamente avvertite, pensiamo al caso di furto di carte di credito in cui è indispensabile avvertire in tempo utile per bloccare la carta chi è stato derubato.

  Il regolamento europeo sulla protezione dei dati (GDPR) verrà applicato a tutte le organizzazioni che operano all'interno dell'Unione Europea e tutte quelle al di fuori che offrono beni o servizi a persone nell'UE e prevede per i cittadini il diritto di cancellazione, limitazione, modifica e portabilità dei dati.

  Per il mancato rispetto del GDPR ossono essere comminate le seguenti sanzioni:

- un'ammonizione scritta in casi di una prima mancata osservanza non intenzionale.
- accertamenti regolari e periodici sulla protezione dei dati
- una multa fino a 20 milioni di euro o fino al 4% del volume d'affari a seconda del tipo di violazione

  Il Gdpr è stato pensato soprattutto per rendere le aziende consapevoli dell'importanza di custodire i dati dei clienti: una gestione non corretta permette anche a un banale virus, preso per aver cliccato sull'email sbagliata, di entrare in un pc e rubare profili che possono poi essere usati per furti d'identità o anche per furti veri e propri nel caso vengano trafugati numeri di carta di credito.

  Per le aziende del turismo questo comporta una serie di obblighi in più che dovranno necessariamente essere individuati da un professionista che deve analizzare i trattamenti dei dati dell'azienda, le precauzioni prese fino ad ora e le misure da intraprendere per adeguarsi alla nuova normativa.