FEDERICO VACCARO
AVVOCATO
0644291081 • info@federicovaccaro.com

Regolamento UE 2016/679 sulla protezione dei dati personali
Cosa sapere e cosa fare

Il Regolamento UE 2016/679

Dal 25 maggio 2018 si applicherà in tutti gli Stati dell'Unione Europea il Regolamento UE 2016/679 (General Data Protection Regulation – GDPR).
Per consentire alle imprese di comprendere di cosa si tratti, individuare quali siano le principali novità introdotte, chiedersi a chi concretamente interessi e interrogarsi sulle motivazioni per cui occorra adeguarsi, abbiamo deciso di predisporre questa brochure informativa sul Regolamento UE 2016/679.

La nostra consulenza tecnico - legale

Siamo un team di avvocati e informatici esperti nel settore della privacy e dell'Information Technology con particolare specializzazione nell'ambito della sicurezza delle soluzioni IT. Attraverso un'esperienza pluriennale maturata nel settore, accompagniamo le imprese lungo il percorso di adeguamento alla normativa europea in materia di protezione dei dati personali.

Le principali novità

Il Regolamento UE 2016/679 richiama alcuni principi e adempimenti già previsti dalla normativa nazionale ma introduce importanti novità, che impongono un ripensamento dei processi e dei sistemi informativi alla base della gestione della privacy e richiedono degli interventi specifici. In particolare il Regolamento:
- Introduce il principio di responsabilizzazione o accountability (art. 5) in base al quale sarà il titolare a decidere, sebbene nei parametri fissati dal Regolamento, con quali misure tecniche o organizzative proteggere i dati, e non solo: oltre che approntare tali misure adeguate ed efficaci il titolare dovrà anche essere in grado di dimostrare la conformità delle attività di trattamento con il Regolamento, compresa l'efficacia delle misure adottate.
- Richiama i principi generali previsti già nel Codice privacy e ne introduce di nuovi – così per i principi della privacy by design e by default (art. 25) che impongono di considerare la protezione dei dati personali fin dalla fase di progettazione, e obbligano i titolari a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.
- Conferma alcuni adempimenti già previsti dal Codice privacy (come ad esempio l'obbligo di fornire agli interessati l'informativa e di gestire il consenso), inserendo alcuni elementi di novità (si pensi ad alcune indicazioni ulteriori sul trattamento che occorre fornire all'interessato attraverso l'informativa, alla sua forma e alle tempistiche in cui va resa).
- Introduce la figura del Data Protection Officer (DPO) o Responsabile della Protezione dei Dati (RPD)– che in alcuni casi è obbligatoria (cfr art. 37).
Prevede la possibilità di nomina dei subresponsabili da parte del responsabile (art. 28).
- Obbliga i titolari e i responsabili a tenere i registri del trattamento, che sostituiscono l'obbligo di notifica all'Autorità.
- Introduce nuovi diritti per l'interessato (si pensi ad esempio al diritto all'oblio e al diritto alla portabilità dei dati trattati con mezzi automatizzati, disciplinati, rispettivamente, agli artt. 17 e 20 del Regolamento).
- Individua l'obbligo di effettuare una preliminare valutazione d'impatto sulla protezione

dei dati personali nei casi in cui il trattamento possa comportare dei rischi (art. 35) e prevede anche la possibilità, se l'esito della valutazione è negativo, di consultare l'autorità di controllo competente affinché indichi come operare.
- Prevede come obbligo generalizzato la comunicazione all'Autorità di eventuali violazioni dei dati personali (data breach), ex art. 33 del GDPR.
- Introduce maggiori responsabilità e prevede un impianto sanzionatorio più rigido, ferme restando le responsabilità penali che continueranno a derivare dalla normativa nazionale.
- Prevede che il titolare e il responsabile debbano adottare le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32), che comprendono, tra le altre, se del caso:
1. la pseudonimizzazione e la cifratura dei dati personali;
2. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
3. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
4. "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento", ovvero, per i sistemi informatici, i penetration test.

A chi interessa
Il Regolamento si rivolge a tutti titolari e i responsabili del trattamento di dati personali. Significa che queste nuove regole devono essere rispettate da tutte le pubbliche amministrazioni, da tutte le imprese e da tutti i professionisti che, nello svolgimento delle loro attività, trattano dati personali, ossia compiono operazioni – come la raccolta, la registrazione, l'organizzazione, la conservazione, l'estrazione, la consultazione– che hanno ad oggetto informazioni relative a persone fisiche, identificate o identificabili. Attenzione, perché non si intende solo nome o cognome: il Regolamento definisce dato personale anche un numero di identificazione, i dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di una persona. Per comprendere quanto sia ampio l'alveo del Regolamento si consideri che rientrano nella definizione di trattamento anche la cancellazione e la distruzione di dati personali.