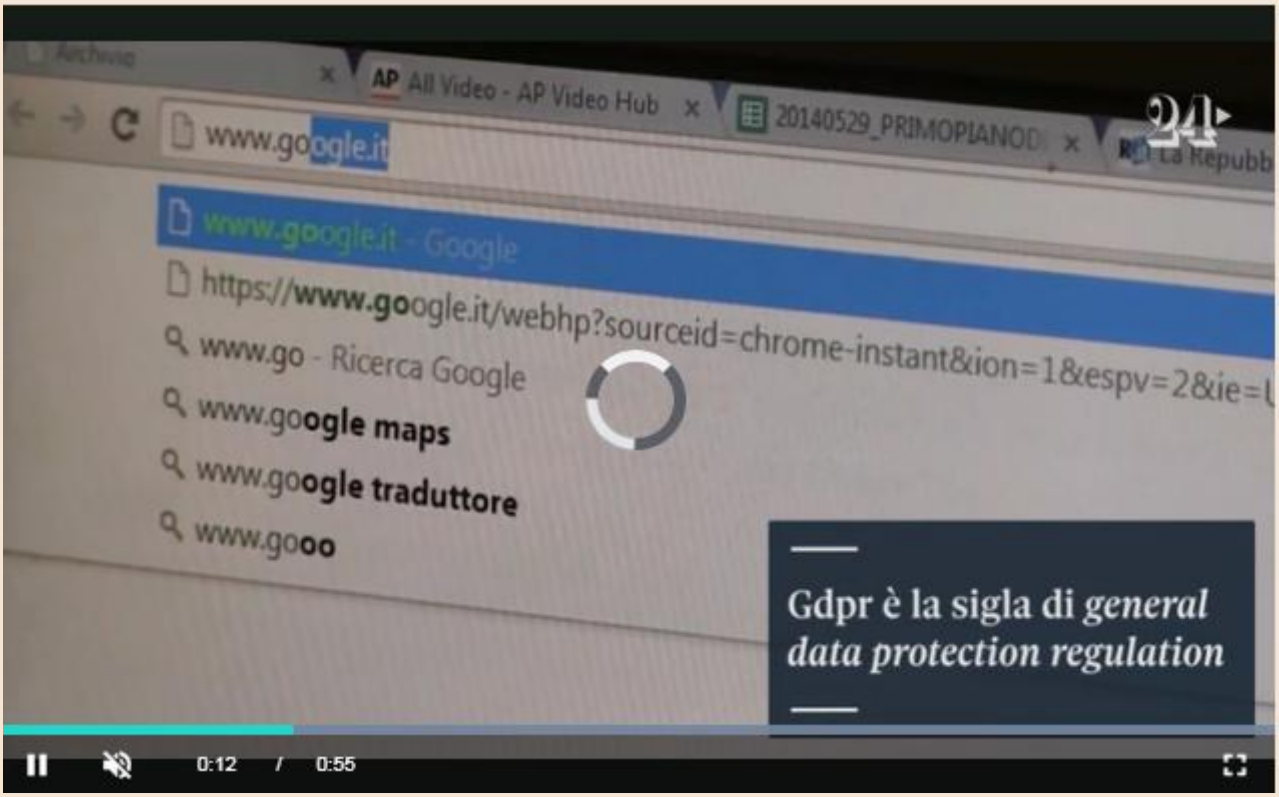
Il Sole 24 ORE

MULTE FINO AL 4% PER LE AZIENDE

# Privacy, che cos'è il Gdpr e perché ci riguarda

–di **Alberto Magnani** | 02 maggio 2018




Più si avvicina, più se ne parla. E si scoprono lacune. Il Gdpr, sigla di *General data protection regulation*, è il regolamento europeo su privacy e dati che diventerà operativo dal 25 maggio 2018. Siamo agli sgoccioli, ma diversi utenti (e aziende) hanno dimostrato di essere in ritardo sulle proprie azioni di adeguamento. È probabile che il Garante per la privacy, l'autorità che vigila sul trattamento dei dati in Italia, conceda un periodo di tolleranza di sei mesi dopo il 25 maggio, comportandosi in maniera più elastica sui casi di infrazione. Ma in cosa consiste, davvero, la Gdpr? È il caso di domandarselo perché, finito il semestre di avvio, si preannunciano multe fino a un massimo di 20 milioni o del 4% sui ricavi annui.

**Prima di tutto... Cosa è un regolamento?**
Il regolamento è uno degli atti legislativi dell'Unione europea, insieme a direttive e decisioni. A differenza di queste ultime, si caratterizza per avere portata generale (vale in tutti i paesi) e applicabilità diretta in tutti i suoi elementi (diventa legge subito, senza dover passare per il recepimento da parte degli Stati membri). I paesi possono decidere di rivedere la propria legislazione se si creano incompatibilità evidenti con le nuove regole europee. Nel caso dell'Italia, ad esempio, si è abolita la parte generale del vecchio Codice della privacy (a sua volta ispirato a una direttiva risalente al 1995) e si sono diluite le restanti norme in un decreto.

**Cosa prevede la Gdpr?**
La Gdpr, come dice la sigla, è un testo che prova a uniformare le leggi europee sul trattamento dati e il (nostro) diritto a essere in pieno controllo delle informazioni che ci riguardano. Il regolamento si compone di 99 articoli e istituisce alcune novità come il diritto all'oblio (gli utenti possono chiedere di rimuovere informazioni a proprio riguardo), la «portabilità» dei dati (si possono scaricare e trasferire dati da una piattaforma all'altra, senza vincolarsi a un certo account) e l'obbligo di notifica in caso di *data breach* (le aziende, se subiscono fughe di informazioni sensibili, devono comunicarlo entro 72 ore). I destinatari sono i «titolari del trattamento», ossia chi gestisce le informazioni: privati e, soprattutto, aziende.

**Quale sarebbe l'impatto su un'azienda "normale"?**
L'impatto è più ampio di quanto si possa pensare, perché la Gdpr riguarda le aziende che gestiscono qualsiasi tipo di dato personale. Dalle informazioni sui propri dipendenti alla profilatura dei clienti per conto terzi: «La Gdpr coinvolge tutte le aziende che trattatano dati - spiega Luca Galetti, consulente della società P4I - Il che può significare le informazioni in mano alle risorse umane sul proprio organico o l'analisi di dati per attività di marketing "targettizzato", mirato su misura a seconda del cliente».

**Quali sono i principali obblighi?**
Fra gli obblighi da tenere in considerazione, Galetti ricorda soprattutto una richiesta di consenso in forma chiara (articolo 7), l'istituzione di un registro delle attività (articolo 30), la notifica delle violazioni entro 72 ore (articolo 33) e la designazione di un «responsabile protezione dati»

(articolo 37). Per quanto riguarda il consenso, l'azienda deve chiedere il via libera «in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro (al contrario delle vecchie e chilometriche informative, *ndr*)». Sul fronte del registro di trattamento, si obbligano i titolari a dotarsi di un registro delle attività dove si elencano - tra le altre cose - le finalità dell'elaborazione dei dati, i destinatari, l'eventuale scadenza per la loro cancellazione.

In caso di *data breach*, la violazione dei propri dati, scattano obblighi di notifica alle autorità molto più stringenti: il titolare deve comunicare l'accaduto «entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche». Infine si va a istitituzionalizzare su scala Ue una figura già accolta da alcune legislazioni: il data protection officer, assunto tra i dipendenti dell'azienda o presso una società esterna con il ruolo di vigilare sull'applicazione effettiva della Gdpr da parte del suo titolare.

**E se si viola il regolamento?**
Se si viola il regolamento, scattano delle sanzioni. Salate. A seconda della gravità dell'infrazione, le multe sono divise in due scaglioni: fino a un massimo di 10 milioni di euro o, per le imprese, il 2% del fatturato (se superiore); oppure fino a un massimo di 20 milioni o il 4% del turnover, sempre per le aziende e sempre in rapporto al giro d'affari. Per farsi un'idea, il Garante alla privacy è riuscito a incassare nel 2015 poco più di 3,3 milioni di sanzioni.
La multa più "leggera" (10 milioni o 2% turnover) viene inflitta per la trasgressione di principi come la *privacy by design* (mancata protezione dei dati fin dalla progettazione) o la carenza di misure adatte a garantire un buon standard di sicurezza. Quella più pesante (20 milioni o 4% del turnover) arriva in caso di violazione dei principi fondamentali, come la negazione del diritto all'oblio o l'opacità nella richiesta di consenso dei dati.

**Non è previsto un periodo di "tolleranza" di sei mesi?**
Non è chiaro. Il Garante alla privacy, a quanto è emerso, dovrebbe allinearsi alla posizione già intrapresa dal suo omologo francese (*Commission nationale de l'informatique et des libertés*) e consentire una specie di stand-by di sei mesi, dove le aziende ritardatarie possono

evitare sanzioni. Ma l’impresa deve comunque mostrare di avere avviato un piano di adeguamento ed essere consapevole delle priorità per rientrare nel perimetro del regolamento.