l regolamento generale sulla protezione dei dati

GDPR (RGPD, in inglese GDPR, General Data Protection Regulation- Regolamento UE 2016/679) è un regolamento con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione europea e dei residenti nell'Unione europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE). Il testo, adottato il 27 aprile 2016, è stato pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, inizierà ad avere efficacia il 25 maggio 2018.

Gli obiettivi principali della Commissione europea nel GDPR sono quelli di restituire ai cittadini il controllo dei propri dati personali e di semplificare il contesto normativo che riguarda gli affari internazionali unificando e rendendo omogenea la normativa privacy dentro l'UE.[1] Dalla sua entrata in vigore, il GDPR sostituirà i contenuti della direttiva sulla protezione dei dati (Direttiva 95/46/EC)[2] e, in Italia, abrogherà le norme del codice per la protezione dei dati personali (dlgs.n. 196/2003) con esso incompatibili.

Riepilogo

"Il regime di protezione dei dati proposto per l'UE estende gli obiettivi della legge europea sulla protezione dei dati a tutte le imprese estere che trattano dati di residenti europei a prescindere dal luogo nel quale le trattano e dalla loro sede legale. Permette di armonizzare le diverse normative sulla protezione dei dati in tutta l'UE, facilitando così l'osservanza delle norme da parte delle imprese non europee; tuttavia, questo è stato ottenuto a costo di un

regime che prevede una severa disciplina di protezione dei dati, con rigide sanzioni che possono raggiungere il 4% del volume globale di affari."[4] A seguito di negoziazioni nel dialogo a tre tra Parlamento Europeo, Commissione europea e Consiglio dei Ministri, si è raggiunto un consenso generale sulla formulazione del GDPR e sulle sanzioni finanziarie per la mancata osservanza.[5]

Ambito

Il regolamento si applica ai dati dei residenti nell'Unione Europea. 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. Ciò anche a prescindere dal luogo o dai luoghi ove sono collocati i sistemi di archiviazione (storage) e di elaborazione (server). Il regolamento non riguarda la gestione di dati personali per attività di sicurezza nazionale o di ordine pubblico ("le autorità competenti per gli scopi di prevenzione, indagine, individuazione e persecuzione di reati penali o esecuzione di provvedimenti penali"). Secondo la Commissione Europea "i dati personali sono qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica. Può riguardare qualunque dato personale: nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer."[8] Il regolamento disciplina solo il trattamento di dati personali delle persone fisiche.

Dati

Vengono ampliate e caratterizzate le definizioni sui dati presenti nella corrente direttiva e aggiunte di nuove. Quindi, oltre al dato personale, troviamo dati genetici, biometrici e relativi alla salute, comunque tutte informazioni che consentono l'identificazione univoca o l'autenticazione di una persona fisica.

- Dato personale: informazioni relative a persona fisica identificata o identificabile. La novità risiede proprio nel criterio di identificazione, dove con “identificativo” si intendono

nome, caratteristiche di tipo fisiche o fisiologiche, identificativo on line.

- Dati genetici: ereditati o acquisiti, ottenuti tramite analisi di DNA ed RNA da un campione biologico della persona fisica in questione.
- Dati biometrici: come l'immagine facciale, grazie ai quali è possibile identificare una ed una sola persona fisica.
- Dati sulla salute: sia fisica che mentale, passata, presente o futura, ma anche informazioni su servizi di assistenza sanitaria, laddove presenti, indipendentemente dalla fonte, quale, ad esempio, un medico.

Sicurezza dei dati

La sicurezza dei dati raccolti è 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. A tal fine il titolare e il responsabile del trattamento garantiscono che chiunque acceda ai dati raccolti lo faccia nel rispetto dei poteri da loro conferiti e dopo essere stato appositamente istruito, salvo che lo richieda il diritto dell'Unione o degli Stati membri (Articolo 32). A garanzia dell'interessato il Regolamento UE 2016/679 regolamenta anche il caso di trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale (Articolo 44 e ss) e prevede che l'interessato venga prontamente informato in presenza di una violazione che metta a rischio i suoi diritti e le sue libertà (Articolo 33).

Responsabile per la protezione dei dati (cd DPO, Data protection officer)

Qualora l'elaborazione sia effettuata da un'autorità pubblica, fatto salvo per le corti o le autorità giudiziarie indipendenti agenti nella loro competenza giudiziaria, o qualora, nel settore privato, l'elaborazione sia effettuata da un controllore le cui attività principali consistono di operazioni di elaborazione che richiedono un monitoraggio regolare e sistematico dei soggetti dei dati, una persona esperta di legislazione e pratiche relative alla protezione

dei dati deve assistere colui che li controlla o li gestisce al fine di verificare l'osservanza interna al regolamento. Il responsabile per la protezione dei dati è una figura simile, ma non identica, al preposto all'osservanza, in quanto ci si aspetta che il primo abbia una buona padronanza dei processi informatici, della sicurezza dei dati (inclusa la gestione dei ciber-attacchi) e di altre questioni di coerenza aziendale riguardanti il mantenimento e l'elaborazione di dati personali e sensibili. Ricorda molto l'Odv (organismo di vigilanza) della legge n. 231 del 2001 sulla responsabilità penale delle persone giuridiche e il responsabile anticorruzioni per la sua autonomia, indipendenza e assenza di conflitti di interesse. L'insieme di competenze richieste si estende al di là della comprensione dell'osservanza legale di leggi e regolamenti sulla protezione dei dati e comporterà una grande preparazione e professionalità. Il monitoraggio dei Data protection office sarà onere del regolatore e non del consiglio di amministrazione dell'organizzazione che assume il funzionario. La nomina di un responsabile per la protezione dei dati all'interno di una grande organizzazione rappresenterà una sfida sia per il consiglio di amministrazione, sia per lo stesso responsabile. Considerati lo scopo e la natura della nomina, sono in gioco una miriade di questioni legate alla governance e a fattori umani che le organizzazioni e le aziende dovranno affrontare. Inoltre, chi detiene l'incarico dovrà creare un proprio team di supporto e sarà anche responsabile del proprio sviluppo professionale continuativo, dal momento che, come "mini-regolatore" ad ogni effetto, dovrà essere indipendente.