Privacy. Dal 25 maggio 2018 entra in vigore il GDPR: cos'è, gli adempimenti e cosa fare

Innanzitutto spieghiamo che cosa è il **GDPR**. La definizione utilizzata dalla Comunità Europea è, naturalmente, in Inglese. GDPR vuol dire General Data Protection Regulation- Regolamento UE 2016/679. in Italiano è RGPD, ovvero "regolamento generale sulla protezione dei dati". Si tratta di 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 provvedimento è stato pubblicato sulla **Gazzetta Ufficiale Europea il 4 maggio 2016** ed è entrato in vigore il 25 maggio dello stesso anno. Tuttavia la sua efficacia avrà inizio il 25 maggio 2018.

I "dati personali" rappresentano il cardine di tutta la normativa, infatti il relativo testo affronta principalmente il tema dell'esportazione di dati personali al di fuori dell' Unione Europea e obbliga tutti i titolari del trattamento dei dati, che si trovano a trattare dati di residenti nell'Unione europea, ad osservare ed adempiere agli obblighi previsti.

Nel GDPR la Commissione Europea ha posto degli obiettivi precisi. Innanzitutto quello di restituire ai cittadini il controllo dei propri dati personali, e poi quello di semplificare il contesto normativo che riguarda gli affari internazionali, unificando e rendendo omogenea la normativa privacy dentro l'Unione Europea

La vecchia direttiva 95/46/EC sulla protezione dei dati, istituita nel 1995, sarà sostituita dal **GDPR** che, in aggiunta, abrogherà le norme del codice per la protezione dei dati personali (**dlgs.n. 196/2003**) che risulteranno con esso incompatibili.

E' pur vero che, con tutta probabilità, questo potrà generare confusione per alcuni, ma bisogna considerare che adesso ci si aspetta che l'Italia ponga una normativa di raccordo che sia in grado di mettere ordine e di inserire le norme del codice privacy non incompatibili all'interno dell'impianto normativo del Regolamento.

Tramite un'altra Direttiva collegata, la **UE 2016/680**, in aggiunta a questo nuovo regolamento, sarà applicata una disciplina speciale e in parte derogatrice per i trattamenti dei dati da parte dell'Autorità Giudiziaria e di tutte le forze di polizia; in ragione della caratteristica dell'istituto della direttiva europea tali trattamenti dei dati (Autorità Giudiziaria e forze di polizia) continueranno ad essere differenti da Stato a Stato ed oggetto di una legislazione separata nazionale .

Questo regime di protezione dei dati proposto per l'Unione Europea 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. Ciò vuol dire che permette di armonizzare le diverse normative sulla protezione dei dati in tutta l'Unione Europea, raggiungendo la finalità di facilitare l'osservanza delle norme da parte delle imprese non europee.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Questo risultato comunque 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**. Tale regime è frutto di una negozazione tra Parlamento Europeo, Commissione europea e Consiglio dei Ministri, raggiungendo il consenso sulla formulazione del GDPR e sulle sanzioni finanziarie per la inosservanza dello stesso.

Ambito
Per quanto riguarda l'Ambito di applicazione del regolamento, esso riguarda i dati dei residenti nell'Unione Europea. Si differisce dall'attuale Direttiva in quanto si applica anche a imprese ed enti, organizzazioni in generale, con sede legale fuori dall'Unione Europea che trattano dati personali di residenti nell'Unione Europea; inoltre si prescinde anche dal luogo o dai luoghi ove sono collocati i sistemi di archiviazione (storage) e di elaborazione (server).

Riguardo ai dati citiamo ciò che afferma 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."

Specifichiamo inoltre due punti importanti da fissare in questa sede:
a) Il regolamento disciplina solo il trattamento di dati personali delle persone fisiche.
b) Il regolamento non riguarda la gestione di dati personali per attività di sicurezza nazionale o di ordine pubblico e, di conseguenza, non coinvolge le autorità competenti per gli scopi di prevenzione, indagine, individuazione e persecuzione di reati penali o esecuzione di provvedimenti penali

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.

Unicità di regole e sportello
A tutti gli stati membri UE si applicherà un insieme unico di regole. Ciascuno stato membro istituirà un'autorità sovrintendente indipendente per dare udienza ai reclami, effettuare indagini, sanzionare le infrazioni amministrative, ecc. Le autorità sovrintendenti in ciascuno stato membro collaboreranno con le altre, fornendo assistenza reciproca e organizzando operazioni congiunte. Qualora una ditta abbia più stabilimenti nell'UE, avrà un'unica autorità sovrintendente come propria "autorità principale", sulla base dell'ubicazione del proprio "stabilimento principale" (ossia il posto dove hanno luogo le principali attività di gestione). L'autorità principale agirà quale "sportello unico" per supervisionare tutte le attività di gestione dati di quella ditta nell'UE (Articoli 46 - 55 del GDPR). Il Comitato europeo della protezione dati (EDPB, European Data Protection Board) coordinerà le autorità sovrintendenti. L'EDPB andrà a sostituire il gruppo di lavoro dell'Articolo 29. Vi sono eccezioni nel caso di dati elaborati in un contesto di impiego e di dati elaborati a scopo di sicurezza nazionale, che potrebbero ancora essere soggetti ai regolamenti delle singole nazioni (Articoli 2(2)(a) e 82 del GDPR)

Responsabilità
Il principio di responsabilità legato al trattamento dei dati personali resta ancorato (come nel Codice per la protezione dei dati personali) ad un concetto di responsabilità per esercizio di attività pericolosa con una valutazione ex ante in concreto ed una sostanziale inversione dell'onere della prova. Per non rispondere del danno commesso derivante dal trattamento dei dati personali occorre sostanzialmente provare di aver fatto tutto il possibile per evitarlo. Il Regolamento aggancia e sviluppa questo tipo di responsabilità verso il concetto di Accountability (art. 5 co. 2). Occorre osservare i principi applicabili al trattamento dei dati personali di cui all'articolo 5 adempiendo alle relative obbligazioni ed essere in grado di comprovarlo.

Consenso
Un valido consenso deve essere esplicitamente dato per la raccolta dei dati e per i propositi per i quali sono usati (Articolo 7; definito in Articolo 4). Pertanto se la richiesta viene inserita nell'ambito di altre dichiarazioni essa va distinta e formulata con linguaggio semplice e chiaro (Articolo 7). Condizione di validità del consenso è che le finalità per cui viene richiesto siano esplicite, legittime, adeguate e pertinenti (Articolo 5). Nel caso in cui il consenso al trattamento dei propri dati personali per una o più specifiche finalità sia stato espresso da minori esso è valido solo se il minore ha almeno 16 anni. L'età viene ridotta a 13 anni solo se lo stato membro ha previsto con legge una diversa età purché non inferiore a questa. Qualora il minore abbia un'età inferiore ai 16 o 13 anni, il consenso al trattamento deve essere dato da un genitore o da chi eserciti la potestà, e deve essere verificabile (Articolo 8). 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 (art. 18).

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

Violazione dei dati (cd Data Breach) art. 33 e art. 34
Il titolare del trattamento dei dati avrà l'obbligo legale di rendere note le fughe di dati all'autorità nazionale e di comunicarle entro 72 ore da quando ne è venuto a conoscenza. I resoconti delle fughe di dati non sono soggetti ad alcuno standard "de minimis" e 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 avvertite.

Segreteria
tel/fax: 085 4714060
mail: info@guardiacivica.it
Posta certificata: info@pec.guardiacivica.it
Skype, Facebook, Twitter: GUARDIACIVICA
CF: 01778600682
IBAN: IT 87 Z 02008 15404 000010644583