E-LEARNING RGPD

IL RGPD PER I PROFESSIONISTI LEGALI: COME AFFRONTARE LA CONFORMITÀ?

Introduzione :

Il Regolamento generale sulla protezione dei dati (noto come "RGPD"), adottato il 14 aprile 2016 ed entrato in vigore il 25 maggio 2018, è stato percepito e sentito come una vera e propria rivoluzione nella protezione dei dati personali e, più in generale, della privacy.

Tuttavia, il RGPD sostituisce o completa vecchi testi i cui principi erano già molto simili: la Direttiva 95/46/CE del 24 ottobre 1995 a livello europeo o, ad esempio, la Loi Informatique et Libertés francese del 6 gennaio 1978.

Ciò che rende il RGPD un testo particolarmente innovativo con un impatto sulle imprese in senso lato è, da un lato, la volontà di uniformare il quadro normativo in materia di protezione dei dati in tutta l'Unione Europea, e anche oltre, e dall'altro il rafforzamento degli obblighi che gravano sulle imprese, accompagnati da sanzioni molto forti.

Questo più ampio ambito di applicazione si riflette nel fatto che il RGPD riguarda tutte le aziende e tutte le organizzazioni pubbliche o private che raccolgono o trattano dati personali in Europa: studi legali, ma anche professionisti legali come notai o ufficiali giudiziari sono quindi tutti interessati dal RGPD nelle loro attività che comportano il trattamento di grandi volumi di dati personali.

In considerazione dei nostri obblighi professionali ed etici, dobbiamo essere particolarmente vigili nel garantire che le nostre attività siano conformi a questi nuovi requisiti.

I. Cosa c'è di nuovo nel RGPD

I.1 Un campo di applicazione più ampio

Gli obiettivi principali del RGPD, ovvero l'armonizzazione delle normative nazionali e il rafforzamento della protezione dei dati personali nel contesto globalizzato in cui vengono trattati, hanno portato a un campo di applicazione notevolmente ampliato:

La nozione di "dati personali" è estremamente ampia, poiché riguarda "*qualsiasi informazione relativa a un interessato*" che corrisponde a "*una persona fisica identificata* [...] *o che può essere identificata, direttamente o indirettamente, con mezzi ragionevolmente utilizzabili dal responsabile del trattamento o da qualsiasi altra persona fisica o giuridica [...*]". Pertanto, i dati personali non sono più definiti solo in termini di natura identificativa delle informazioni in possesso del responsabile del trattamento stesso, ma anche in termini di possibilità che tali informazioni possano

essere incrociate con altre informazioni in possesso di terzi, conferendo loro una natura identificativa.

Inoltre, la definizione di dati anonimi o pseudonimi contenuta nel GDPR è estremamente restrittiva. In sostanza, non appena i dati sono suscettibili di essere individualizzati, anche se non identificano direttamente una persona, rientrano nell'ambito dei dati personali.

Ad esempio, elaborando statistiche pseudonimizzate sulle preferenze dei propri clienti o conservando documenti relativi a un caso che non riportano il nome o il cognome di una persona... i dati personali vengono trattati a priori e il RGPD deve essere rispettato.

L'ambito territoriale di applicazione del RGPD è ampio: non appena un trattamento viene effettuato nel contesto delle attività di uno stabilimento situato nel territorio dell'Unione Europea, riguardante un residente europeo o collegato a un'offerta di beni o servizi a persone situate nel territorio dell'Unione Europea, si applica il RGPD. Allo stesso modo, il trasferimento di dati al di fuori dell'Unione Europea o l'accesso ai dati dall'esterno di questo territorio è soggetto a regole molto severe che tendono a essere rafforzate sotto l'influenza della Commissione Europea.

È comprensibile, nel contesto dell'uso costante di strumenti digitali e nuove tecnologie e in cui i dati personali stanno diventando una forte posta in gioco economica: il RGPD si applica ovunque e sempre!

II.2 Obblighi rafforzati

Il RGPD richiede alle aziende di ripensare la loro organizzazione della gestione e della protezione dei dati personali, in particolare attraverso :

L'obbligo per tutte le aziende, tranne in alcuni casi, **di tenere un registro** con l'elenco dei trattamenti effettuati. Questo registro deve mostrare un certo numero di informazioni che richiedono di sapere esattamente quali dati vengono trattati e come. Questo lavoro può sembrare noioso, ma spesso consente un'analisi approfondita che facilita la conformità al RGPD in un secondo momento.

L'obbligo di definire la **ripartizione delle responsabilità con i propri fornitori di servizi o partner:** il RGPD prevede diverse qualifiche (responsabile del trattamento, contitolare del trattamento o incaricato del trattamento) che dipendono da chi decide i mezzi e le finalità del trattamento dei dati personali. La distribuzione di queste responsabilità deve essere contrattualizzata in un documento che rispetti un certo numero di disposizioni imposte dal RGPD.

- Può essere obbligatorio o raccomandato nominare un "**responsabile della protezione dei dati**", il cosiddetto "DPO", che è la pietra miliare della conformità al RGPD.

- I principi di minimizzazione e proporzionalità introdotti dal RGPD richiedono anche di definire per **quali periodi di tempo i dati vengono conservati** (indipendentemente dal supporto: cartaceo o digitale). Queste "politiche di

conservazione dei dati" devono essere affidabili e basate su criteri chiari, come le finalità per cui i dati vengono utilizzati (non dovrei conservare dati di cui non ho bisogno), gli obblighi di legge o i periodi di prescrizione applicabili.

Il GDPR pone inoltre un forte accento sull'implementazione delle **misure necessarie, sia tecniche che organizzative, per garantire un adeguato livello di sicurezza dei dati trattati**. Ciò include anche l'obbligo di notificare all'autorità di vigilanza nazionale le perdite e le violazioni gravi di dati personali entro 72 ore dalla scoperta della violazione, generalizzato a tutte le organizzazioni. Inoltre, se la violazione può incidere sulla privacy delle persone interessate, anche queste dovranno essere informate.

Il RGPD ha cambiato le aspettative delle aziende e delle organizzazioni che trattano i dati: se prima, come in Francia, era sufficiente rilasciare semplici dichiarazioni alla Commission Nationale Informatique et Libertés, ora è richiesta una conoscenza approfondita delle operazioni di trattamento effettuate e la documentazione di come vengono soddisfatti i requisiti normativi.

III.3. Maggiore tutela dei diritti delle persone interessate

La natura protettiva del RGPD si riflette in un rafforzamento dei diritti degli interessati. Pertanto, oltre ai diritti esistenti, come il diritto di accesso o il diritto di rettifica, esistono nuovi diritti che gli interessati possono esercitare nei confronti delle aziende:

L'estensione del **diritto all'informazione** (articoli 13 e 14 del RGPD): oltre agli elementi di informazione già previsti dal regolamento precedente, le informazioni fornite alle persone fisiche devono riguardare, in particolare, anche "la durata del periodo di conservazione" e "qualsiasi altra informazione necessaria per garantire un trattamento corretto dei dati", il che è molto ampio.

Consenso (articoli 4 e 7 del GDPR): Ove richiesto, il consenso dovrà essere esplicito e distinto. In altre parole, le persone devono dare il consenso per ogni utilizzo dei loro dati per cui è richiesto. Inoltre, il GDPR introduce requisiti specifici di consenso per i minori di 16 anni per la fornitura di determinati servizi.

Il diritto alla **cancellazione** o "diritto all'oblio" (articolo 17 del GDPR): Gli interessati possono richiedere la cancellazione dei propri dati in diversi casi, in particolare quando i dati non saranno più necessari per le finalità per cui sono stati raccolti o trattati o quando le persone desiderano ritirare il proprio consenso o opporsi al trattamento.

Il diritto alla **portabilità (**articolo 20 del GDPR): I responsabili del trattamento devono consentire la comunicazione dei dati di una persona interessata a un altro responsabile del trattamento in un formato "strutturato, di uso comune e leggibile".

La gestione delle richieste di esercizio dei diritti da parte degli interessati deve essere anticipata per poter rispondere in modo completo ed entro i termini imposti dal RGPD. Ad esempio, per quanto riguarda il diritto all'informazione, ciò significa esaminare le note informative o l'informativa sulla privacy sul sito web o su qualsiasi altro supporto attraverso il quale vengono raccolti i dati. Allo stesso modo, per poter rispondere a una richiesta di diritto di accesso, si raccomanda di prevedere una procedura volta a

individuare quali dati devono o possono essere trasmessi e come estrarre dai propri sistemi informativi volumi di dati che possono essere significativi.

Per garantire l'osservanza di questi obblighi e per fornire alle autorità di tutela delle leve reali contro le aziende che controllano, il GDPR ha aggiunto **sanzioni amministrative, il cui** importo è stato notevolmente aumentato. A seconda del tipo di violazione, la multa può arrivare a 20.000.000 di euro o fino al 4% del fatturato mondiale annuo, se superiore. L'arsenale delle sanzioni prevede anche la possibilità per le autorità di vigilanza di rendere pubbliche le loro decisioni, il che ha un forte impatto e quindi un deterrente per le imprese sanzionate.

II. Le principali azioni di conformità

Quali sono le fasi principali?

1. **Definire la governance**: per affrontare la compliance in modo appropriato e razionale, si raccomanda di :
    - Definire se è obbligatorio o rilevante nominare un DPO e identificare gli attori strategici interni e/o esterni per garantire la conformità;
    - Condurre campagne di sensibilizzazione interne per diffondere le buone pratiche e garantire l'efficacia dell'approccio.

2. **Inventariare le operazioni di trattamento**: questa fase è essenziale per adattare le misure di conformità e garantire la realizzazione di un registro completo. A tal fine, è spesso utile iniziare a raccogliere e analizzare l'eventuale documentazione esistente (registro, vecchie dichiarazioni CNIL, ecc.) prima di inventariare le principali categorie di trattamento per progetto e/o finalità (clienti, risorse umane, fornitori di servizi IT, ecc.).

3. **Definire le priorità delle azioni da realizzare**: è necessario **stabilire un calendario che tenga conto di :**
    - Attività, dimensioni e struttura dei team coinvolti ;
    - Possibili fattori esterni che possono avere un impatto sulle azioni prioritarie da realizzare (ad es. un nuovo progetto in corso o da avviare).

4. **Garantire la conformità**:

Tutte queste azioni possono essere implementate quando sono necessarie, in base alle priorità specifiche di ogni attività.