Informativa su Regolamento UE/2016/679

General Data Protection Regulation (GDPR)

Alla luce dell'imminente entrata in vigore del Regolamento UE numero 679 del 2016, e della mancata emanazione da parte del Governo di una normativa specifica finalizzata ad armonizzare il contenuto del Regolamento con la normativa nazionale vigente, lo Studio Ferrari & Associati ritiene, nel Vostro interesse, di fornire un breve documento informativo (non esaustivo in ragione dell'estrema complessità della materia) per l'individuazione di alcuni temi da tenere in considerazione nella valutazione delle attività da adottare al fine di adeguare, per quanto ad ora possibile, le propria attività alle vincolanti e stringenti richieste emanate dall'Unione Europea in tema di protezione della Privacy.

Cos'è il GDPR

Il General Data Protection Regulation, è un atto normativo emanato dal Parlamento europeo e dal Consiglio dell'Unione Europea, direttamente applicabile nei Paesi membri a partire dal prossimo **25 maggio 2018**.

A norma del Art. 1 primo e terzo comma del Regolamento, l'oggetto e le finalità dello stesso sono rappresentate dalla "**protezione delle persone fisiche con riguardo al trattamento dei dati personali**" e dal garantire la "libera circolazione dei dati personali nell'Unione".

Al fine di permettere ciò vengono dettate una serie di indicazioni e norme che in sostanza stabiliscono il diritto delle persone fisiche di:

1. **ricevere informazioni chiare** rispetto alle modalità e finalità di trattamento dei loro dati personali
2. il diritto di poter **richiedere informazioni** rispetto all'effettivo utilizzo di tali dati
3. il diritto a richiedere la "**portabilità**" dei propri dati personali
4. esercitare il "diritto all'**oblio**" (difficile pensare di poter esercitare un simile diritto in ambito negoziale e commerciale, visti gli obblighi di conservazione dei documenti e dei dati da parte dei professionisti in ragione di tutela propria e dei propri assistiti o di tutela dell'imprenditore rispetto a pretese avanzate da clienti o fornitori, sempre e comunque previsti dalla normativa).

La garanzia che un'impresa o un'associazione professionale può prestare verso i propri Clienti e verso le Autorità vigilanti è rappresentata dalla figura del **Responsabile della Protezione dei Dati** o Data Protection Officer (**DPO**), figura richiamata all'Art 37 del Regolamento, che dovrebbe rappresentare il responsabile dell'adozione e dell'implementazione di una **adeguata struttura organizzativa finalizzata alla protezione** di ogni tipologia possibile di **dati** relativi a **persone fisiche individuate** od **individuabili** (Art. 4).

Le **sanzioni** previste in caso di mancato adeguamento e del rispetto di tali prescrizioni possono risultare particolarmente gravi, essendo state fissate sanzioni (queste certe, al contrario di qualunque altro aspetto di questa disciplina) che possono arrivare al 4% del fatturato fino a 20 milioni di euro.

Chi lo deve applicare

La risposta è **tutti**.

Stabilire chi sia effettivamente tenuto, e con quali modalità, all'applicazione delle complesse previsioni del regolamento è un punto dirimente rispetto alla **responsabilità** che l'impresa o l'associazione si assume di fronte ai **Clienti** ed all'**Autorità** di vigilanza (nel caso di specie il Garante per la Protezione dei Dati Personali o **Garante Privacy**) ed alle conseguenti azioni da adottare.

L'elemento centrale della disciplina in oggetto è rappresentata dall'***Accountability***, termine con il quale si fa riferimento alla responsabilizzazione dell'impresa e del professionista, rispetto alla rischiosità delle proprie attività in termini di gestione di dati sensibili ed all'adozione di "misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento" (Art. 24)

Stabilire chi sia tenuto, ed in che misura, all'adozione delle prescrizioni del Regolamento, permette di distinguere tra un Soggetto tenuto ad adottare: uno specifico Modello Organizzativo (attraverso la designazione di personale dedicato e procedure organizzative specifiche), il Registro delle attività di trattamento, la nomina con contestuale comunicazione al Garante del Responsabile della Protezione dei Dati, e chi invece può di fatto **limitarsi** ad adottare le **previsioni già esistenti ed obbligatorie nel sistema normativo nazionale dal 1995** in avanti (ultimo ed organico riferimento, applicabile fino al 24 maggio 2018, il D.Lgs. 196/2003, o Codice Privacy).

Al di là della responsabilizzazione e dalla previsione di autovalutazione del rischio richiesta dal Regolamento, lo stesso fornisce una "indicazione" rispetto alla determinazione dell'obbligatorietà o meno della nomina e conseguente comunicazione al Garante della privacy del Responsabile della Protezione dei Dati.

Nello specifico, all'Art. 37 comma 1 viene stabilito che: "Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogni qualvolta:

a) il trattamento è effettuato da un'**autorità pubblica** o da un **organismo pubblico**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare** e **sistematico** degli interessati su **larga scala**; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su **larga scala**, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10."

Purtroppo il Regolamento non fornisce alcuna indicazione di cosa si intenda per "larga scala" come dei concetti di "monitoraggio regolare e sistematico", viene quindi rimessa all'autonomia decisionale del responsabile dell'azienda la determinazione di se e quando tale fattispecie si concretizzi, prendendo comunque a riferimento le indicazioni fornite dal Gruppo di Lavoro ex Articolo 29, costituito in seno alla Commissione Europea.

Elemento certo è che la procedura più rilevante da adottare, anche in considerazione del fatto che in prima istanza si tratta dell'unico adempimento formalmente indirizzato ad un Ente Pubblico (e quindi immediatamente contestabile), nel caso in cui si ritenga effettivamente di trovarsi nelle condizioni di applicabilità del citato Articolo 37, è la **nomina** e **comunicazione** al Garante della Privacy del nominativo del Responsabile.

Cosa cambia rispetto a prima

Rispetto a quanto previsto dalla normativa sulla privacy ad oggi vigente, le differenze immediatamente rilevanti per chiunque operi al di fuori della sfera privata, sono rappresentate dalla necessità di fornire agli interessati la possibilità di richiedere il trasferimento dei propri dati sensibili e la comunicazione del nominativo di un referente per l'Autorità e per gli interessati (sia il Responsabile di cui all'Art 37, che il "punto di contatto" indicato e consigliato fra gli altri dal Documento emanato dal CNDCEC) considerato che ai sensi dell'Art.7 del D.Lgs. 196/2003 (**Codice Privacy**) era già previsto che:

"L'interessato ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza" e così via dicendo.

Nel caso in cui invece il Titolare del trattamento dei dati (chi determina le finalità e i mezzi del trattamento di dati personali, di solito il responsabile dell'attività), ravveda la sussistenza di situazioni tali da richiedere la nomina del Responsabile della Protezione dei Dati, l'azienda dovrà dotarsi di specifici Modelli Organizzativi, sistemi di controllo ed unità operative.

In caso si verifichino delle **violazioni** nel protocollo e si rilevi una **perdita** e/o un **furto di dati** (*Data Breach*), sarà necessario procedere a comunicare tale violazione senza indugio (e comunque entro 72 ore) al Garante.

COME SI FA

Come espresso già in premessa, l'adozione di adeguate modalità di tutela dei dati sensibili in ossequio alle previsioni del Regolamento n.679 del 2016 è un'attività tutt'alto che semplice, che richiede un'adeguata valutazione delle caratteristiche specifiche dell'attività svolta, e di conseguenza della tipologia e mole di dati manipolati.

Tra l'altro le attività di cui sopra non risultano di semplice implementazione, stante la mancata adozione di provvedimenti normativi e codici di condotta da parte delle Istituzioni, come invece auspicato ed indicato dallo stesso Regolamento (e.g. Artt. 40; 35; 57).

Effettuiamo quindi una macro suddivisione per distinguere tra quegli interventi che, in ragione delle previsioni introdotte già dal D.Lgs. 196/2003 e successive modificazioni, saranno ragionevolmente già state adottate da ciascuno (che richiedono solo minimi accorgimenti) e quegli interventi ritenuti più gravosi, indicati e ritenuti vincolanti solo per soggetti che possano essere considerati come più vulnerabili o comunque atti a manipolare una significativa quantità di informazioni sensibili.

Indicazioni generalmente applicabili:

1. Anzitutto (sembra una banalità ma potrebbe sfuggire) sostituire nei Vostri moduli relativi alle autorizzazioni al trattamento dei dati personali i **riferimenti normativi** (non più D.Lgs. 196/2003 ma Regolamento UE/2016/679) integrandoli con alcune **informazioni rilevanti** (vedi punto successivo);

2. In fase di stipula di un contratto con un Cliente che preveda la raccolta di dati di carattere personale, richiedere **espressamente il consenso al trattamento dei dati** ed illustrare i **diritti** dell'interessato nel rispetto di quanto previsto dal Regolamento, congiuntamente all'indicazione del **nominativo** (questa la prima vera novità) del Punto di contatto o del Responsabile della Protezione dei Dati quando nominato. Tali previsioni si applicano anche alle icone standardizzate utilizzate sui siti web delle organizzazioni;

3. La **pseudonimizzazione** e la **cifratura** dei dati personali (ad esempio associando un numero per ciascun cliente, creando un archivio nel quale registrare le associazioni ed utilizzare esclusivamente tale numero per nominare fascicoli facilmente accessibili nei locali dell'attività);

4. Adottare misure di sicurezza di tipo **informatico** utilizzando ad esempio **Password** e **cifrature di dati**, creando cartelle con permessi di accesso diversificati ed

adottando **programmi** che abbiano delle **certificazioni** rispetto al rispetto dei requisiti di sicurezza informatica;

5. Effettuare regolarmente il **backup** dei dati in maniera tale da garantire l'accessibilità delle informazioni in caso di perdita o distruzione di tali dati dai sistemi operativi principali;

6. La responsabilizzazione del personale sulle procedure e sul rispetto della riservatezza delle informazioni delle quali sono entrati in possesso in ragione del loro ruolo;

7. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il **titolare del trattamento** effettua, prima di procedere al trattamento, **una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali**.

In particolare sul procedimento di definizione del rischio, il Garante suggerisce il ricorso ad un software di analisi sviluppato dal **CNIL**, l'Autorità francese per la protezione dei dati, al seguente link http://www.garanteprivacy.it/web/guest/regolamentoue/dpia#STRUMENTI .

Bisogna tenere a mente che la responsabilità di decidere in che misura e con quali modalità applicare tali procedure ricade in capo al Titolare ed al Responsabile "sempre tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (Art.32).

Indicazioni per i soggetti obbligati a nominare un RPD o DPO:

1. Nominare formalmente un Responsabile per la Protezione dei Dati attraverso il protocollo indicato al sito https://servizi.gpdp.it/comunicazione-rpd/ , per la quale si avvisa, viene richiesto il possesso di una firma digitale;

2. Stabilire delle procedure di aggiornamento continuativo adottate dal Responsabile;

3. Istituire (sempre, quando l'organizzazione abbia più di 250 dipendenti) un Registro delle attività di trattamento di cui all'Art. 30.

In sostanza per chi si trovasse già in regola con le previsioni vigenti da prima dell'introduzione del GDPR, le attività operative da porre in atto sono prossime a nessuna, per chi invece si trovasse in difetto rispetto all'applicazione di talune indicazioni questa rappresenta un'opportunità (diciamo pure obbligata) di provvedere a regolarizzare la propria situazione.

Per chi si trovasse invece nella situazione di dover applicare ulteriori previsioni rispetto a quanto già indicato dalla normativa del 2003, il Regolamento rappresenta ragione di sensibile irrigidimento delle procedure da adottare e di responsabilizzazione rispetto ad un aspetto ad oggi forse un po' sottovalutato.

Il **consiglio** è quello di procedere comunque con una autovalutazione del rischio, indicando, nel caso in cui si stabilisca di non voler comunicare il Nominativo del Responsabile per la Protezione dei dati, le ragioni per la quali non si ritiene di dover applicare tali previsioni (tipologia dei dati trattati, applicabilità e sostenibilità di tali procedure, effettiva inesistenza di un trattamento su larga scala). Il tutto al fine di rispettare il citato principio di ***Accountability*** grazie al quale si può, entro certi limiti, stabilire in autonomia le procedure più adeguate da adottare che, vedete bene, non corrisponde al non adottare alcun tipo di valutazione.

Lo **Studio Ferrari & Associati**, nell'augurarsi di aver fornito uno strumento utile al fine di comprendere la tematica ed eventualmente aver fornito uno spunto per applicare ed implementare nuove procedure utili al fine di adeguare la propria struttura alle esistenti nonché alle nuove procedure, rimane a disposizione per chiarimenti ed approfondimenti.