studiofasulo

Milano, 16/4/2018

Il nuovo GDPR – General Data Protection Regulation

Il **25 Maggio 2018 entra in vigore** (al termine di un periodo di "moratoria" pro adeguamento, infatti la sua emanazione è datata 24 maggio 2016) e verrà applicato in tutti i Paesi Europei **il nuovo Regolamento Generale sulla Protezione dei Dati (GDPR - General Data Protection Regulation)** pubblicato sulla Gazzetta Ufficiale Europea il 4 Maggio 2016. (Regol. 2016/679)
Il Regolamento obbliga a rivedere le misure di sicurezza e a disporre nuove forme di verifica e controllo che integrano o si aggiungono a quanto disposto dal D.Lgs. 196/2003 attualmente in vigore e che non viene abrogato.
Sono previste sanzioni amministrative pecuniarie dal 2% al 4% del fatturato annuo oltre a sanzioni penali disposte dagli Stati membri.

Obbligo di Adeguamento

I titolari di una azienda, di attività commerciali o di studi professionali, hanno l'obbligo di adeguarsi al nuovo regolamento ed adottare nuove responsabilità in materia di **consenso, protezione e trattamento dei dati**. Dal 25 Maggio 2018 saranno assoggettati ad un **nuovo regime di responsabilità** per tutti i dati personali e le informazioni private, pubbliche e professionali relative ad una persona: **nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer e qualsiasi altra informazione riguardante una persona fisica identificata o identificabile. *(c.d. interessato).***

Principali novità

- **Obbligo di condurre una DPIA – (Data Protection Impact Assessment) (art.35 del Regolamento U.E.)** quando un trattamento dati (o più trattamenti) può presentare un elevato rischio per i diritti e le libertà delle persone fisiche. Procedura volta a valutare la necessità, la proporzionalità e i rischi di un singolo trattamento al fine di adottare misure idonee al rispetto delle prescrizioni normative.
- **Privacy by design e Privacy by default**
- **Obbligo di istituzione del registro dei trattamenti** nei casi prescritti dalla norma.
- **Obbligo di nomina di un RDP (DPO**) Responsabile della protezione (se richiesto).

giuseppe fasulo
ragioniere commercialista revisore dei conti
20146 milano, via roncaglia 14
tel 02.48014111 fax 02.43412461
e-mail: g. fasulo@pdpdue.com
pec: giuseppe.fasulo@lamiapec.it
c.f.: FSLGPP54T19F205F p.iva: 06957780156

studiofasulo

- **Diritto all'oblio**
- **Portabilità dei dati**
- **Trasferimento dei dati all'estero**
- **Garante Europeo**
- **Sanzioni**

DPIA: cos'è, importanza, responsabilità

- E' di competenza del titolare del trattamento.
- E' un processo di analisi che il titolare deve compiere qualora i trattamenti, specie se prevedono in particolare l'uso di nuove tecnologie, possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
- È volta a descrivere le attività di trattamento, valutandone necessità e proporzionalità e determinandone l'origine, la natura, la particolarità e la gravità del rischio connesso
- può essere affidata ad altri soggetti non necessariamente interni all'organizzazione aziendale.
- è obbligo del titolare monitorarne lo svolgimento eventualmente per il tramite dell'RPD (Responsabile della protezione – DPO in inglese) e coordinandosi con il responsabile IT.
- deve essere condotta prima di procedere ad un qualsivoglia trattamento e deve essere assoggettata ad un continuo riesame, con valutazioni ad intervalli regolari (AUDIT).
- Aiuta e guida il titolare, oltre che al rispetto delle prescrizioni del GDPR, anche ad attestare di aver adottato misure idonee a garantire gli interessati in relazione al trattamento dei loro dati personali.
- E' è una procedura volta a valutare e dimostrare la conformità con la normativa in materia di protezione dei dati personali.
- Le prescrizioni, trattate dal Gruppo di lavoro Art. 29, suggeriscono di valutarne l'impiego anche laddove il Regolamento non la prescrive come obbligatoria.

DPIA obbligatoria se ricorrono almeno due criteri fissati dal GDPR

- trattamenti che implichino la valutazione dell'interessato, la Sua profilazione e il suo *SCORING;*

giuseppe fasulo
ragioniere commercialista revisore dei conti
20146 milano, via roncaglia 14
tel 02.48014111 fax 02.43412461
e-mail: g. fasulo@pdpdue.com
pec: giuseppe.fasulo@lamiapec.it
c.f.: FSLGPP54T19F205F p.iva: 06957780156

- la conclusione di contratti in modo automatizzato (es. mutui, assicurazioni, viaggi, tickets etc.);
- il monitoraggio degli interessati (es. videosorveglianza o ad esempio *log-books* interni dai quali si evincano costantemente le abitudini degli interessati od anche meta-data delle fotografie, o *logs* di geolocalizzazione);
- dati relativi a soggetti (ritenuti) vulnerabili (anziani, minori, soggetti con patologie psichiatriche);
- dati sensibili, giudiziari o di natura estremamente personale;
- dati trattati su larga scala;
- utilizzo di soluzioni tecnologiche e organizzative innovative (es. acquisizione di foto, riconoscimento del volto, applicazioni IoT, metatags di foto; dati genetici e biometrici);
- trattamenti di dati che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. screening di una banca attraverso dati registrati in una centrale rischi per stabilire la concessione di un mutuo)

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, **eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio** *(si veda art. 30, paragrafo 5)*, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Consenso – Art. 4 (11) – 7 - 8

- Consenso dell'interessato: è qualsiasi manifestazione di volontà, libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio consenso, mediante dichiarazione o azione positiva inequivocabile che i dati personali che lo riguardano siano oggetto di trattamento.

giuseppe fasulo
ragioniere commercialista revisore dei conti
20146 milano, via roncaglia 14
tel 02.48014111 fax 02.43412461
e-mail: g. fasulo@pdpdue.com
pec: giuseppe.fasulo@lamiapec.it
c.f.: FSLGPP54T19F205F p.iva: 06957780156

- Per i dati "sensibili" (si veda art. 9 regolamento) il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).
- Non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.
- Il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Informativa – Art. 13 - COSA CAMBIA

I contenuti dell'informativa sono più ampi rispetto al Codice L.196/2003.

Il titolare DEVE SEMPRE:

- specificare i dati di contatto del RPD-DPO ove esistente,
- la base giuridica del trattamento,
- qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento,
- se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione,
- il diritto di presentare un reclamo all'autorità di controllo.
- se il trattamento comporta processi decisionali automatizzati la logica di tali processi decisionali e le conseguenze previste per l'interessato.
- Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

GDPR – cosa fare in pratica

- Valutazione impatto DPIA

giuseppe fasulo
ragioniere commercialista revisore dei conti
20146 milano, via roncaglia 14
tel 02.48014111 fax 02.43412461
e-mail: g. fasulo@pdpdue.com
pec: giuseppe.fasulo@lamiapec.it
c.f.: FSLGPP54T19F205F p.iva: 06957780156

studiofasulo

- Puntuale profilazione del cliente tramite *check list* e questionari
- Identificazione dei soggetti (titolari, referenti, responsabili, DPO)
- Verifica dei luoghi dove i dati (anche fisici) vengono archiviati (ed eventualmente distrutti)
- Audit informatico (informativa ai dipendenti sull'uso delle mail e delle informazioni riservate – adozione di sistemi di messaggistica criptata e repository di dati sicuri e certificati – prove simulate di *backup* e *restore* e *disaster recovery*)
- Interviste al personale
- Rilascio di documento di valutazione (e identificazione del rischio)
- Adozione di codici di condotta
- Adozione di procedure interne (specie in caso di DATA BREACH – violazione, perdita dei dati), di comunicazione dell'evento ai soggetti interessati / Garante)
- Verificare sovrapposizioni con **ISO 27001**

giuseppe fasulo
ragioniere commercialista revisore dei conti
20146 milano, via roncaglia 14
tel 02.48014111 fax 02.43412461
e-mail: g. fasulo@pdpdue.com
pec: giuseppe.fasulo@lamiapec.it
c.f.: FSLGPP54T19F205F p.iva: 06957780156