Confartigianato

Confartigianato IMPRESE FIRENZE

Nuovo regolamento europeo sulla Privacy (N°679/2016/UE) - GDPR -

In vigore dal 25 maggio 2018

Seminario informativo – 06 Luglio 2018

Ultimi step normativi in materia di Privacy

- In sintesi:
  - La normativa nazionale era «ferma» al D. Lgs. N° 196/2003 cd. «Codice Privacy»
  - Il 24 maggio 2016 è entrato in vigore il Nuovo regolamento Europeo sulla Privacy **679/2016** «General Data Protection Regulation» (**GDPR**) che deve essere applicato in tutti i paesi UE a partire dal **25 maggio 2018** per uniformare la disciplina in materia degli stati membri
  - L'art. 13 della L. 163/2017 ha delegato il Governo all'emanazione di un Decreto di adeguamento del quadro normativo nazionale alle disposizioni contenute nel **Regolamento UE 679/2016** che in sintesi prevede l'abrogazione del D. Lgs. N° 196/2003 e la costituzione di un nuovo Codice Privacy richiamando le disposizioni del **Regolamento UE 679/2016** ed inserendo specifiche disposizioni.

- **Trattamento dei dati**:
  - Qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione.

- **Dato personale**:
  - **Qualsiasi informazione riguardante una persona fisica identificata o identificabile** ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale..

- **Dato personale** (categorie particolari):

- Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- Dati giudiziari: relativi alle condanne penali e ai reati o a connesse misure di sicurezza

- **Titolare del trattamento**:
  - La persona fisica o giuridica, l’Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell’Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

- **Responsabile del trattamento**:
  - La persona fisica o giuridica, l’Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

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

- **Violazione dei dati personali**:
  - La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.

- **Oggetto e finalità (art. 1)**:
  - Oggetto e finalità: Il presente regolamento stabilisce norme relative alla **protezione delle persone fisiche con riguardo al trattamento dei dati personali**, nonché norme relative alla **libera circolazione** di tali dati.
  - L'introduzione del citato Regolamento UE n. 679/2016 sul trattamento dei dati ha, come scopo principale, l'armonizzazione delle regole sul trattamento dei dati in tutta l'Unione Europea.
  - Infatti, se precedentemente all'introduzione del Regolamento l'applicabilità della legge era definita considerando la sede del Titolare, con la nuova normativa si dovrà considerare la residenza del cittadino all'interno dei confini europei.

- **Principi applicabili al trattamento (art. 5)**:
  - Liceità – Correttezza – Trasparenza
  - Limitazione delle finalità: determinate, esplicite e legittime
  - Minimizzazione dei dati: adeguati, pertinenti e limitati a quanto necessario secondo le finalità
  - Esattezza e aggiornamento
  - Limitazione della conservazione: per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
  - Integrità e riservatezza: trattati in maniera da garantire un'adeguata sicurezza dei dati personali

- **Principio di accountability (art. 5 c. 2)**:
  - La nuova impostazione, in riferimento all'utilizzo di **dati** ed **informazioni**, si basa sostanzialmente su un approccio che vuole arrivare alla **massima riduzione del rischio per la libertà e la dignità del cittadino**
  - In tal senso è stato introdotto il **principio di accountability**, inteso quale "**responsabilizzazione**" assieme ad un concomitante **obbligo di rendicontazione delle misure** intraprese per essere coerenti con il nuovo impianto normativo.
  - **L'obbligo di dimostrare il rispetto della normativa**, posto in capo al Titolare del trattamento, è già, di per sé stesso, una garanzia di rispetto della norma imponendo un passaggio da una protezione meramente formale ad una **protezione sostanziale** generata dalla necessità di dover **dimostrare**, nel corso del tempo, **l'adozione di misure realmente efficaci**.

- **Liceità del trattamento (art. 6)**:

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi (cfr. considerando 47), a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti).

Privacy by design: necessità di tutelare il dato **sin dalla progettazione** di sistemi informatici che ne prevedano l'utilizzo

Art 25, c 1 Regolamento UE: Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e tutelare i diritti degli interessati.

Privacy by default: necessità, **per impostazione predefinita**, di trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario.

Art 25, c.2 Regolamento UE: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità

In sintesi:

- Mutare i processi organizzativi in vista della tutela e riduzione del rischio può essere alquanto laborioso ed oneroso sia dal punto di vista organizzativo che economico.
- Occorre individuare un processo strutturato che tocchi una serie di punti, quali:
  - Ricognizione ed **identificazione dei trattamenti di dati personali**, che potrà, poi sfociare nella predisposizione del **registro dei trattamenti** svolti.
  - Individuare le unità aziendali che se ne occupano con la **mappatura dei soggetti da autorizzare**.
  - **Individuazione dei rischi che incombono sui dati**, che potrà eventualmente sfociare nella predisposizione di una **valutazione di impatto dei trattamenti** (DPIA) e la conseguente adozione di contromisure adeguate.
  - Non sarà quindi più sufficiente intendere la protezione del dato come sistema statico, ma sarà necessario procedere a **valutazioni periodiche** dell'esistente e ad **analisi preventive** in caso di introduzione di nuove tipologie di trattamento.
  - Sarà quindi necessario dotarsi di **procedure interne organizzate e standardizzate** che consentano il monitoraggio di ogni fase di trattamento nell'ottica della riduzione del rischio e l'organizzazione di **momenti formativi** per i soggetti autorizzati (obbligatori ex art. 29, Regolamento UE n. 679/2016).