FOGLIO INFORMATIVO SULLA PRIVACY

Regolamento UE sulla protezione dei dati personali Nr. 679/2016

Il Regolamento UE sulla protezione dei dati personali nr. 679/2016 (di seguito „Regolamento UE“) entra in vigore direttamente in tutta l'Unione Europea il 25 maggio 2018. Fino a tale data tutti i trattamenti di dati personali devono essere adeguati alla nuova normativa.

INDICE

Maggiore responsabilizzazione del titolare del trattamento

Il titolare del trattamento, e cioè, colui che determina i mezzi e le finalità del trattamento, è responsabile per garantire il rispetto dei principi giuridici applicabili a tutti i trattamenti posti in essere dall'organizzazione e ad egli incombe l'onere di provare il rispettivo rispetto. Il titolare del trattamento è il punto di riferimento sia per le persone interessate sia per l'autorità di controllo. Tale responsabilità non può essere delegata, neppure attraverso un'eventuale nomina di un responsabile per la protezione dei dati (il cosiddetto DPO).

Nei casi in cui sia nominato un responsabile del trattamento esterno (p.es. un cloud-provider o un amministratore IT esterno), incombe allo stesso titolare del trattamento di assicurare che tale soggetto esterno presenti garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento EU, anche per la sicurezza del trattamento.

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

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.

Registro delle attività di trattamento

Sebbene non tutte le organizzazioni sono obbligate alla tenuta di un registro delle attività di trattamento, esso è comunque parte centrale e punto di partenza di tutte le riflessioni relative alla protezione dei dati personali all'interno di un'organizzazione.

Attraverso il registro si crea la mappatura analitica di tutti i flussi di dati personali. Il registro evidenzia (a) i canali attraverso i quali i dati personali confluiscono all'interno dell'organizzazione, (b) cosa succede poi all'interno dell'organizzazione con tali dati, ed infine (c) i soggetti esterni ai quali i dati vengono trasferiti.

A tal fine, ogni trattamento di dati (p.es. marketing, contabilità salariale, video-sorveglianza) viene analizzato in linea di principio sulla base dei seguenti criteri: (a) finalità del trattamento, (b) descrizione delle categorie di dati trattati, (c) categorie di persone interessate, (d) categorie di destinatari dei dati, (e) periodo di conservazione massimo dei dati, nonché (f) una descrizione generale delle misure di sicurezza tecniche ed organizzative poste in essere per la tutela dei dati.

Consenso della persona interessata al trattamento dei dati

In alcuni casi, il consenso della persona interessata al trattamento dei dati è obbligatorio. Questo è il caso in linea generale sempre quando il trattamento rappresenta un rischio elevato per la tutela della sfera privata dell'interessato. Ove sussiste questo rischio elevato, il legislatore ha optato per il rafforzamento del potere di controllo dell'interessato attraverso l'obbligatorietà del consenso prestato dalla stessa.

Il Regolamento UE prevede tale obbligatorietà nei seguenti casi (e l'onere di provare che il consenso è stato validamente conferito verte sul titolare del trattamento):

- nei casi in cui il trattamento riguarda le cosiddette categorie particolari di dati (vedasi art. 9 del Regolamento UE);

- nei casi in cui dati personali vengono trasferiti dal titolare in paesi terzi rispetto alla UE/SEE, e con rispetto a tali paesi terzi la Commissione Europea non ha deciso che garantiscono un livello di protezione dei dati personali adeguato;
- nei casi in cui il titolare del trattamento intende sottoporre l'interessato ad una decisione basata unicamente sul trattamento automatizzato – compresa la profilazione – che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;
- alcune ipotesi di marketing diretto particolarmente invasive (l'interessato può comunque ed in ogni caso opporsi al marketing diretto);
- ecc.

Violazione dei dati personali

Una violazione dei dati personali consiste nella distruzione, nella perdita, nella modifica, nella divulgazione non autorizzata o nell'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Notifica di una violazione dei dati personali all'autorità di controllo: In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Comunicazione di una violazione dei dati personali all'interessato: Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Valutazione d'impatto sulla protezione dei dati

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.

Una valutazione d'impatto sulla protezione dei dati è sempre consigliabile. Nei seguenti casi descritti in maniera sommaria, tale valutazione è prescritta dalla legge:

- valutazione sistematica e globale di aspetti personali relativi a persone fisiche;

- trattamento, su larga scala, di categorie particolari di dati personali, come p.es. dati personali che rivelino l'origine razziale o etnica (per un elenco esaustivo, vedasi art 9.1 del Regolamento UE), o di dati relativi a condanne penali e a reati;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Responsabile della protezione dei dati

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

- 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
- 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.

Il responsabile della protezione dei dati non può essere rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Egli svolge tra le altre cose i seguenti compiti: (a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE, (b) sorvegliare l'osservanza del Regolamento UE, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, (c) cooperare e fungere da punto di contatto per l’autorità di controllo e per le persone interessate.

Diritto di essere informato e diritti delle persone interessate

Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta dell’interessato senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa.

I diritti fondamentali delle persone interessate sono i seguenti:

- Diritto di accesso dell'interessato (quali dati vengono trattai per quali finalità? ecc.);
- Diritto di rettifica di dati inesatti;
- Diritto alla cancellazione («diritto all'oblio»);
- Diritto di limitazione di trattamento (p.es. opposizione al marketing diretto);

- Diritto di essere informato dal titolare in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;
- Diritto alla portabilità dei dati;
- Diritto di opposizione al trattamento.

Poteri dell'autorità di controllo – pene edittali elevate

Alcuni poteri importanti dell'autorità di controllo (www.garanteprivacy.it/) sono:

- ingiungere al titolare del trattamento di fornire ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;
- condurre indagini sotto forma di attività di revisione sulla protezione dei dati;
- ottenere dal titolare del trattamento l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti (compreso l'accesso a tutti i locali del titolare);
- rivolgere avvertimenti/ ammonimenti al titolare del trattamento;
- imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
- ecc.

Pene edittali elevate: Il Regolamento EU prevede espressamente che le sanzioni inflitte a chi viola la normativa debbano essere *effettive, proporzionate e dissuasive*.

Per l'inosservanza del Regolamento UE la nuova normativa prevede in casi particolarmente severi sanzioni amministrative pecuniarie fino a 20.000.000,00 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.