GDPR REGOLAMENTO EUROPEO 679/16

FAQ

NORMATIVA

Cos'è il nuovo Regolamento Europeo?

Regolamento Europeo 2016/679 è il testo per la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Tra le misure privacy da adottare nel rispetto del Regolamento Europeo 679, c'è l'obbligo di predisporre le misure organizzative e tecnologiche per garantire la sicurezza dei dati personali trattati.
L'individuazione delle misure da intraprendere è onere del titolare del trattamento o del responsabile, se dallo stesso Titolare nominato.
Viene richiesto anche di cooperare con l'autorità di controllo notificando qualsiasi violazione dei dati personali alla stessa e al diretto interessato entro 72 ore dal momento in cui se ne è venuti a conoscenza, all'autorità di controllo competente, e senza ingiustificato ritardo secondo l'art. 33.

Cos'è l'ACCOUNTABILITY?

Con applicazione in tutti gli Stati Membri (a partire dal 25 maggio 2018) del regolamento Privacy 679, i Titolari e Responsabili del trattamento dovranno seguire il "principio della accountability" (art. 5 co. 2) che comporterà l'onere di dimostrare l'adozione, senza convenzionalismi, di tutte le misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Regolamento (art. 24-25 e l'intero CAPO IV). La dimostrazione riguarda, quindi, sia gli assett documentali che quelli tecnologici che la rendicontazione della formazione acquisita in materia da parte di tutti i soggetti coinvolti nel trattamento dei dati.

Quando sarà l'esecutivo?

I regolamenti UE, per loro natura intrinseca, sono immediatamente esecutivi e non richiedendo la necessità di recepimento da parte degli Stati Membri e garantiscono una maggiore armonizzazione a livello dell'intera UE. Ragion per cui il regolamento europeo è già esecutivo dalla data di emanazione (25 maggio 2016)

Cosa è la portabilità?

L'obiettivo del Regolamento 2016/679 è quello di rafforzare il controllo sui propri dati personali quando questi sono trattati con mezzi automatizzati:
ricevendo tutti i dati personali che lo riguardano in un formato strutturato, di uso comune e leggibile da dispositivo automatico e interoperabile; trasmettendoli, se necessario, ad un altro fornitore di servizi o titolare del trattamento; facendoli trasmettere direttamente da un titolare all'altro, se tecnicamente possibile.
Si applica solo dietro consenso o se la stessa è necessaria per l'esecuzione di un contratto.
L'informativa deve contenere la possibilità per l'interessato di richiedere la portabilità dei suoi dati

Il GDPR si occupa di videosorveglianza?

Il Regolamento 679 si occupa di videosorveglianza stabilendo che il titolare del trattamento è tenuto a procedere con un preventivo data protection impact assesment (DPIA) ex art. 35 Regolamento UE 2016/679 nelle ipotesi di sorveglianza sistematica su larga scala di zona accessibile al pubblico.
Restano ad oggi fermi i provvedimenti del Garante italiano in materia.
Chi fa uso della videosorveglianza, deve effettuare, nel rispetto del principio di proporzionalità, la scelta e le modalità della ripresa e la dislocazione delle telecamere affinché le stesse registrino i dati pertinenti e non eccedenti allo scopo della ripresa stessa.
Ad esempio l'angolo di visuale della ripresa deve essere limitato ai soli spazi di esclusiva pertinenza, escludendo ogni registrazione audio-video di aree comuni, o ancora i soggetti interessati dalle riprese

devono essere informati con apposita cartellonistica (visibile anche in orario notturno) e avvisati che stanno accedendo ad una zona video sorvegliata.
Alla “videosorveglianza“che le persone fisiche fanno per scopi esclusivamente personali (videocitofono, sistema di ripresa di sicurezza, etc.) se non viene condivisa/diffusa sistematicamente con terzi e non vengono rese pubbliche le riprese, non si applica la normativa Privacy.

TERMINOLOGIA

Cosa si intende per consenso?
Il “consenso” è la libera indicazione della volontà del soggetto interessato di accettare esplicitamente una specifica operazione di trattamento relativa ai propri dati personali, di cui era stato informato in anticipo da colui che ha il potere di decidere su tale elaborazione (il Titolare del trattamento).
Il Regolamento UE 2016/679 tratta negli articoli 7 e 8 il “consenso” quale onere della prova della sussistenza del consenso al trattamento prestato dall’interessato è in capo al titolare.
In qualsiasi momento l’interessato può revocare il proprio consenso, senza che questo pregiudichi la liceità del trattamento già effettuato precedentemente.
Il trattamento dei dati del minore è lecito solo se questo abbia almeno 16 anni (in alcuni stati anche 13), altrimenti è necessario il consenso prestato o autorizzato dal titolare della responsabilità genitoriale.
Il GDPR prevede che il consenso sia GRANULARE ED ESPLICITO; ne deriva quindi l’impossibilità di richiedere, con un’unica firma e/o click su modulo web, il consenso per diverse finalità. (esempi: bisogna richiedere un flag separato per finalità commerciali, finalità di erogazione del servizio, finalità di profilazione, finalità di comunicazione a terzi etc..)

Cosa si intende per dato sensibile?
Il dato sensibile è il dato personale che, per sua natura, richiede particolare attenzione: i dati sensibili rivelano origine razziale o etnica, credenze religiose o altre convinzioni, opinioni politiche, tesseramento a partiti, sindacati o associazioni, salute e vita sessuale.

Cosa si intende per informativa?

L’informativa è un avviso contenente le informazioni che il Titolare del trattamento è tenuto a fornire a tutti gli interessati, sia per via orale che per iscritto, in modo chiaro conciso, in merito a quando e come i dati vengono raccolti sia direttamente dall’Interessato che tramite terzi, e come gli stessi vengono utilizzati. È la base giuridica che ti consente di effettuare il trattamento in maniera lecita.

Cosa si intende per profilazione?

Qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l’affidabilità, il comportamento, l’ubicazione o gli spostamenti della persona fisica. Per questa attività il consenso deve essere esplicito.

Cosa si intende per pseudonimizzazione?

Il trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti ad un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona identificata o identificabile. La pseudonimizzazione si rende necessaria soprattutto nei casi di dati particolarmente sensibili.

SOGGETTI COINVOLTI

Chi sono i destinatari del GDPR?

Il Regolamento Europeo è entrato in vigore il 25 maggio 2016 e si applicherà in tutti gli Stati Membri a partire dal 25 maggio 2018, termine entro il quale le aziende dovranno adeguarsi alla nuova legge sulla privacy. Il regolamento europeo si rivolge a tutte le aziende, attività **professionali presenti negli Stati dell’Unione Europea e a tutte quelle sedi che, pur trovandosi fuori dai confini europei, svolgono**

un'attività di trattamento dati di individui che si trovano in UE in relazione all'offerta di beni e servizi anche non remunerati e ad attività di monitoraggio del comportamento.

Chi sono i soggetti principali in ambito privacy?

principali soggetti della Privacy sono: l'interessato, il titolare del trattamento dei dati, il Responsabile del trattamento, il DPO, il terzo e l'Autorità di Controllo.

Interessato:
la persona fisica cui si riferiscono i dati personali.

Titolare del Trattamento:
La persona fisica, la società, l'associazione o un'altra entità che controlla il trattamento dei dati personali ed è autorizzata a prendere decisioni essenziali sulle finalità e modalità di tale trattamento, comprese le misure di sicurezza applicabili.

Responsabile del Trattamento:
la persona fisica, la società, l'associazione o l'organizzazione a cui il Titolare ha affidato l'attività specifica di gestione e controllo dei dati personali, in base all'esperienza e/o alle competenze pertinenti in materia.

DPO (Data Protection Officer):
il professionista con conoscenze specialistiche sulla legislazione e sulle pratiche in materia di protezione dei dati.
Egli è designato dal Titolare / Responsabile in tre occasioni:

- il trattamento è effettuato da un'autorità pubblica;
- il trattamento è su larga scala e coinvolge dati sensibili;
- il trattamento richiede un controllo regolare e sistematico degli Interessati.

Terzo:
la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento. E' una persona autorizzata al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.

Autorità di Controllo:
L'autorità pubblica indipendente istituita da uno Stato membro www.garanteprivacy.it

Quando è obbligatorio nominare un DPO?

Secondo l'art. 37 del GDPR, la nomina di un "responsabile alla protezione dei dati" è sempre obbligatoria per il settore pubblico e per il settore privato, invece, con riferimento alle grandi imprese o alle imprese che effettuato trattamenti a rischio (ad esempio trattamento su larga scala di dati sensibili, monitoraggio regolare e sistematico degli interessati su larga scala).
Il gruppo di lavoro dei garanti europei WP29 ha emanato delle linee guida che chiariscono i concetti di larga scala e monitoraggio regolare e sistematico: ne sono alcuni esempi, gli istituti di videosorveglianza, le ztl, gli ipermercati che usufruiscono di fidelity card, le cliniche mediche e comunque tutte quelle aziende che attraverso il trattamento dei dati hanno una gestione continua e costante del dato stesso e del ciclo di vita del dato.

Il DPO deve essere interno o esterno?

Secondo il regolamento europeo privacy 679, la designazione del "Data Protection Officer" può essere affidata a personale interno o esterno di un'azienda con comprovate capacità in aree giuridiche e informatiche (art. 37 comma 5 e 6). Egli avrà il compito di analizzare, valutare e disciplinare la gestione del trattamento dei dati personali e della loro gestione/salvaguardia all'interno dell'azienda, secondo le direttive imposte dalle normative vigenti (art. 39).
Può inoltre essere nominato anche fra i dipendenti del responsabile del trattamento, se esterno.

Chi è il contitolare?

Il Contitolare del Trattamento è una persona fisica o giuridica, che affianca il Titolare e a cui competono diverse responsabilità decise tramite accordo interno (art.26).
L'accordo tra le parti, redatto in forma libera, deve riflettere in modo puntuale i ruoli reciproci (art.26.2), il riparto degli obblighi previsti dal Regolamento (art. 26.1), il rapporto reciproco nel confronto degli interessati (art. 26.2), come ad esempio in materia di riscontro e di fornitura dell'informativa (art. 26.1) e

sebbene non direttamente accessibile nella sua totalità deve essere conosciuto dall'interessato il contenuto essenziale ma risulta inopponibile all'interessato che può rivolgersi a chi vuole.

Esiste ancora l'incaricato al trattamento dei dati personali?

A differenza che nel Codice Privacy, il nuovo Regolamento UE non utilizza espressamente il termine «incaricato», ma fa confluire in «terzo» chiunque sia sotto l'autorità diretta del Titolare o del Responsabile (art. 10, n. 10). Le funzioni rimangono comunque immutate.

DIRITTI DEGLI INTERESSATI

Cos'è il diritto all'oblio?

Con l'applicazione da parte in tutti gli Stati Membri del regolamento Privacy 679, ogni individuo potrà richiedere la cancellazione dei propri dati in possesso di terzi (per motivazioni legittime) come previsto dall'art. 17 del GDPR. Questo potrà accadere, ad esempio, in ambito web quando un utente richiederà l'eliminazione dei propri dati in possesso di un social network o di altro servizio web. Si ricorda, ad ogni modo, che il diritto di richiedere la cancellazione dei dati personali in qualunque momento incontra il limite relativo ai documenti di natura fiscale per i quali si seguono comunque gli obblighi conservativi di 10 anni.

Quali sono i diritti concessi agli interessati?

Il Regolamento europeo dà un ampio spazio ai diritti dell'interessato rispetto al passato, ed un intero capo del regolamento europeo è dedicato a tale argomento.

- Diritti di natura conoscitiva:
  - Diritto all'informativa;
  - Diritto di accesso;
  - Diritto alla comunicazione di una violazione dei dati.
- Diritti di controllo:
  - Consenso al trattamento;
  - Diritto di limitazione del trattamento;
  - Revoca del consenso al trattamento;
  - Diritto di opposizione al trattamento;
  - Diritto alla portabilità dei dati;
  - Diritto di rettifica ed integrazione;
  - Diritto alla cancellazione e all'oblio;
  - Decisioni basate unicamente su trattamento automatizzato.
- In particolare ha assunto rilievo il cosiddetto **diritto all'oblio** (art. 17):
  - diritto di veder cancellati i propri dati personali presso il titolare che li tratta;
  - diritto di veder cancellati i rinvii a questi dati, che potrebbero apparire sui motori di ricerca più diffusi.
- Il diritto ad «essere dimenticati» deve concordarsi con il diritto di informazione e di libera espressione (si pensi ad un fatto di cronaca in cui è coinvolto l'interessato), e in generale con l'interesse pubblico e con eventuali obblighi legali.
- Pertanto l'interessato non sempre potrà richiedere la cancellazione immediata dei dati che lo riguardano (riportati ad esempio da un sito web) fintanto che tali dati avranno una rilevanza pubblica, stante ovviamente la correttezza degli stessi.
- L'interessato ha diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano se sussiste uno dei seguenti motivi:
- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti;
- l'interessato revoca il consenso;
- l'interessato si oppone al trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere ad un obbligo legale.
- Il diritto alla cancellazione non si applica se il trattamento è necessario:

- all’esercizio del diritto alla libertà di espressione e di informazione;
- per l’adempimento all’obbligo legale che richieda il trattamento previsto dal diritto dell’unione o dello stato membro cui è soggetto il titolare del trattamento, o per l’esecuzione di un compito svolto nel pubblico interesse oppure nell’esercizio di pubblici poteri;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
- per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria.
- L’interessato ha il diritto di ottenere la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
- contesta l’esattezza dei dati personali;
- il trattamento è illecito e l’interessato si oppone alla cancellazione e chiede, invece, che ne sia limitato l’utilizzo;
- benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all’interessato in sede giudiziaria;
- l’interessato si è opposto al trattamento, in attesa della verifica in merito alla eventuale verifica della prevalenza dei motivi legittimi del titolare del trattamento.
- Se il trattamento è limitato, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell’interessato o per l’accertamento di un diritto in sede giudiziale, o per motivi di interesse pubblico