PRIVACY

Il nuovo Regolamento europeo 2016/679

Soggetti - Adempimenti - Sanzioni

Studio legale Chiodi
info@studiolegalechiodi.com

Fonti normative

- Codice della Privacy (D.lgs 196/2003):
  - disposizioni generali (artt 1-45)
  - disposizioni relative a specifici settori (artt 46-140)
  - tutela dell'interessato e sanzioni (artt 141-186)

- Regolamento UE 2016/679: relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Strumenti interpretativi

- Provvedimenti Autorità Garante
- Vademecum 2013 Autorità Garante

Regolamento UE 2016/679

Costituito da 99 articoli, preceduti da 173 «considerando»

- Art 1

Stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché norme relative alla libera circolazione di tali dati.

Protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali

- Art 94

Abroga la Direttiva 95/46 CE (c.d. Dir. madre) a decorrere dal 25 Maggio 2018

- Art 99

A decorrere dal 25 Maggio 2018, è obbligatorio e si applica direttamente in ciascuno degli Stati membri

Le principali novità introdotte dal Regolamento UE 679/16

- Nuove definizioni per i principali istituti
- Introduzione di nuovi principi generali
- Introduzione di nuove figure: il Data Protection Officer
- Informativa all'interessato rafforzata
- La valutazione di impatto per la protezione dati
- Registro delle attività di trattamento e *data breach*
- I diritti dell'interessato: diritto all'oblio ed alla portabilità dei dati
- Nuovo apparato sanzionatorio

Definizioni

Trattamento dati

Art 4: 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

Art 4: 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

Principi generali

- Art 5 Principi applicabili al trattamento

  a) Liceità – Correttezza - Trasparenza

  b) Limitazione delle finalità: determinate, esplicite e legittime

  c) Minimizzazione dei dati: adeguati, pertinenti e limitati a quanto necessario secondo le finalità *(Vademecum: informazioni personali pertinenti e non eccedenti)*

  d) Esattezza e aggiornamento

  e) Limitazione della conservazione: per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (*Vademecum: conservazione registrazioni per 24-48 ore*)

  f) Integrità e riservatezza: trattati in maniera da garantire un'adeguata sicurezza dei dati personali

  comma 2: Principio di accountability: Il titolare del trattamento è competente per il rispetto del paragrafo 1 e deve essere in grado di comprovarlo («responsabilizzazione»)

Adempimenti Privacy

- Conferimento dell'incarico ai Soggetti Privacy
- Informativa all'interessato ed eventuale raccolta del consenso
- Adozione di misure adeguate di protezione dei propri strumenti informatici e dei luoghi di conservazione dati

- Se sussistono i requisiti:
  - Registri delle attività di trattamento
  - Valutazione di impatto su protezione dei dati

- In ipotesi di *data breach*
  - Notifica all'Autorità di controllo
  - Notifica all'interessato

I soggetti della privacy

- Interessato

- Titolare del trattamento: centro di imputazione giuridica del trattamento, determina finalità e mezzi del trattamento
- Responsabile del trattamento: preposto dal Titolare al trattamento dei dati personali per conto del Titolare
- Incaricato del trattamento: autorizzato a compiere operazioni di trattamento dal Titolare o dal Responsabile. La nomina è obbligatoria, effettuata mediante lettera di designazione.
- Amministratore di sistema: gestione e manutenzione di un impianto di elaborazione
- Data protection officer

- Autorità di controllo: autorità pubbliche indipendenti incaricate dal singolo Stato membro a sorvegliare il rispetto del Regolamento (strumenti di tutela: reclamo – ricorso giurisdizionale nei confronti dell'Autorità o nei confronti del Titolare o del Responsabile del trattamento)

I diritti dell'Interessato

- Art 15 – Diritto di accesso: ottenere dal titolare del trattamento conferma che sia in corso un trattamento di dati personali che lo riguardano e in tal caso, l'accesso a dati personali e informazioni (finalità, categorie di dati, destinatari, periodo di conservazione, diritto di rettifica/ cancellazione dei dati o limitazione /opposizione al trattamento, diritto di proporre reclamo, informazioni su origine dati, esistenza di un processo decisionale automatizzato)

  Vademecum: accesso del condomino ai soli dati a lui riferibili (ed ovviamente alla intera gestione)

- Art 16 Diritto di rettifica e integrazione dei dati
- Art 17 Diritto alla cancellazione (diritto all'oblio) nei seguenti casi: dati non più necessari/ revoca del consenso/opposizione al trattamento/dati trattati illecitamente/per obbligo legale/offerta diretta di servizi della società dell'informazione a minori (Art 8)
- Art 18 Diritto di limitazione del trattamento
- Art 20 Diritto alla portabilità dei dati: ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali forniti a un titolare del trattamento e diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti, qualora il trattamento si basi sul consenso o su un contratto oppure il trattamento sia effettuato con mezzi automatizzati
- Art 21 Diritto di opposizione al trattamento dei dati personali
- Art 22 Processo decisionale automatizzato: diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici o che incida in modo analogo significativamente sulla persona

Responsabile del Trattamento

Art 4: soggetto che tratta i dati personali per conto del Titolare del trattamento

Vademecum Autorità garante:

- l'Assemblea può designare l'amministratore attribuendogli uno specifico ruolo in materia di privacy
- I dati raccolti mediante videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza che ne consentano l'accesso alle sole persone autorizzate

Art 28 Regolamento UE:

- Garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate
- I trattamenti del Responsabile sono disciplinati da un contratto
- Il Responsabile può nominare suoi responsabili previa autorizzazione scritta del Titolare

La nuova figura del Data Protection Officer

Art 37 Regolamento UE: prevede la nomina del responsabile della protezione dei dati quando:

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.

Il DPO è designato in funzione delle qualità professionali (conoscenza specialistica della normativa e delle prassi in materia) e della capacità di assolvere i compiti di cui all'articolo 39.

Può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Funzioni: informare e fornire consulenza, sorvegliare l'osservanza della normativa e le politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati, cooperare con l'Autorità di controllo e fungere da punto di contatto con la stessa.

Informativa nel Regolamento UE

Art 13: Informazioni da fornire in ipotesi di dati raccolti presso l'interessato

Finalità e le modalità del trattamento, natura obbligatoria o facoltativa del conferimento, conseguenze di un eventuale rifiuto di rispondere, i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza, i diritti dell'interessato, gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile

Informazioni aggiuntive rispetto all'Art 13 del Codice Privacy: dati di contatto del titolare del trattamento (e ove applicabile del suo rappresentante), dati di contatto del responsabile della protezione dei dati (DPO), base giuridica del trattamento; i legittimi interessi perseguiti dal titolare del trattamento o da terzi; ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione.

Nel momento in cui i dati personali sono ottenuti, ulteriori informazioni:

a) il periodo di conservazione o i criteri utilizzati per determinare tale periodo;

b) I diritti di accesso ai dati personali, di rettifica, di cancellazione degli stessi, di limitazione del trattamento, di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

e) natura legale o contrattuale dell'obbligo di comunicazione, possibili conseguenze della mancata comunicazione di tali dati;

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Informativa nel Regolamento UE

Art 14: dati non ottenuti presso l'interessato, informazioni in merito a:

La fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico e le categorie di dati personali oggetto di trattamento;

Per dati non raccolti presso l'interessato, l'informativa dovrà essere fornita al più tardi entro un mese dall'ottenimento dei dati o, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato o con un terzo, al più tardi al momento di tale comunicazione.

La comunicazione non è necessaria se l'interessato ha già le informazioni, impossibile/sforzo sproporzionato, comunicazione/ottenimento obbligo di legge, riservati per obblighi di segreto professionale

Il consenso nel Regolamento UE

Art 4 - 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

Art 6 – il consenso dell'interessato costituisce una delle condizioni di liceità del trattamento

Altre condizioni di liceità: esecuzione di un contratto, adempimento obbligo legale, salvaguardia interessi vitali dell'interessato, compito di interesse pubblico o connesso a pubblici poteri, legittimo interesse del titolare o di terzi

Art 7 – Condizioni per il consenso

- Il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso
- La richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie/questioni, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro
- Diritto di revocare il proprio consenso in qualsiasi momento, con la stessa facilità con cui è accordato
- Nel valutare se il consenso sia stato liberamente prestato, si tiene in considerazione l'eventualità che l'esecuzione di un contratto sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Informativa e consenso nel Regolamento UE

Art 8 Condizioni applicabili al consenso dei minori

Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dai genitori.

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

Art 9 Trattamento di categorie particolari di dati

Vieta il trattamento dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il divieto non trova applicazione nei casi di consenso esplicito, obblighi e diritti in materia di diritto del lavoro/sicurezza sociale/protezione sociale, interesse vitale di soggetto con incapacità fisica o giuridica di prestare il proprio consenso, effettuato da fondazione, associazione o altro organismo senza scopo di lucro per membri ed ex membri, dati personali resi manifestamente pubblici dall'interessato, necessario per accertare/esercitare/difendere un diritto in sede giudiziaria o dalle autorità in funzioni giurisdizionali, necessario per motivi di interesse pubblico rilevante, finalità di medicina preventiva o di medicina del lavoro, motivi di interesse pubblico nel settore della sanità Pubblica, necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica/storica o a fini statistici

Registri delle attività e notificazione

Art 37 Codice Privacy: stabilisce quando il titolare deve procedere alla notifica del trattamento al Garante (es. dati genetici, biometrici, di geolocalizzazione, idonei a rivelare lo stato di salute e la vita sessuale, dati volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, dati relativi al rischio sulla solvibilità economica).

Il Regolamento UE sostituisce tale obbligo con:

Art 30 Reg. UE: registri delle attività di trattamento

Sono tenuti ogni titolare e ogni responsabile di trattamento per imprese /organizzazioni con più di 250 dipendenti, oppure chi effettua trattamento che possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (Art 9, p. 1) o i dati personali relativi a condanne penali e a reati (Art 10)

Art 33 Reg. UE: obbligo di notifica all'Autorità di controllo dei casi di violazione dei dati personali (Data Breach) -> senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Art 34 Reg. UE: notifica all'interessato qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Valutazione di impatto su protezione dei dati

Art 35 Regolamento UE: introduce la necessità di procedere ad una valutazione di impatto 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

Tale valutazione è richiesta in caso di:

a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione,

b) trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Nuovo apparato sanzionatorio previsto dal Regolamento UE

Art 82: diritto al risarcimento del danno materiale o immateriale causato dalla violazione del Regolamento

Art 83: Sanzioni amministrative pecuniarie:

- fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente: es. violazioni condizioni applicabili al consenso dei minori (Art 8)/mancata tenuta dei registri delle attività del trattamento (Art 30)
- fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente: es. trattamento di categorie particolari di dati personali, al di fuori degli esoneri dal divieto (art. 9) / trattamento di dati senza aver reso adeguata informativa (art. 13);

Nell'irrogazione della sanzione l'Autorità deve tener conto di molteplici fattori (es. la natura, la gravità e la durata della violazione, il carattere doloso o colposo della violazione; le misure adottate per attenuare il danno; il grado di responsabilità del titolare del trattamento o del responsabile del trattamento, eventuali precedenti violazioni, il grado di cooperazione con l'Autorità di controllo, le categorie di dati personali interessate dalla violazione, etc)