REGOLAMENTO U.E. 2016/679

NOVITÀ LEGISLATIVE IN MATERIA DI PROTEZIONE DEI DATI

Realizzato da :

Studio
Avv. Nizza
& associati

Reg. U.E. 679/2016 approvato il 27.04.2016 entra in vigore il 25.05.2018

L'entrata in vigore del nuovo regolamento comunitario comporta la disapplicazione automatica delle norme interne non conformi (codice della privacy D.Lgs. 196/2003) in attesa di un intervento del legislatore nazionale

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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»*

Studio
Avv. Nizza
& associati

Trattamento:

«*qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a 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*»

Principali novità

Studio
Avv. Nizza
& associati

I. FONDAMENTO DI LICEITÀ

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; **i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice della privacy:**

a) Consenso per una o più specifiche finalità,

b) adempimento obblighi contrattuali,

c) interessi vitali della persona interessata o di terzi,

d) obblighi di legge cui è soggetto il titolare,

e) Interesse pubblico o esercizio di pubblici poteri,

f) interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati

È vietato il trattamento di determinate categorie di dati:

«*dati che rivelino l'origine raziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*» (c.d. «dati sensibili e sensibilissimi per il cod. privacy) – art. 9

N.B. è **ammesso** nei casi previsti dallo stesso art. 9, tra cui:

- Consenso espresso
- Trattamento effettuato nell'ambito delle sue legittime attività e con adeguate garanzie da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato

È stato eliminato il meccanismo previsto dal cod. privacy della notifica all'autorità garante e della autorizzazione.

a) Consenso:

«*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*»

- Non deve necessariamente essere documentato per iscritto né è richiesta la forma scritta

Però la modalità scritta può essere preferibile in quanto idonea a configurare l'inequivocabilità del consenso ed a consentire al titolare del trattamento di fornire la prova che il consenso è stato validamente prestato (art. 7)

- La formula utilizzata per richiedere il consenso deve essere comprensibile, semplice e chiara. Inoltre deve essere chiaramente distinguibile da altre richieste (ad es. se inserita all'interno di un modulo)
- Non è ammesso il consenso tacito o presunto: non saranno più valide la caselle da spuntare sui moduli
- Il consenso viene rilasciato esclusivamente per la/e finalità specificate
- Il consenso dei minori è valido a partire dai 16 anni (il limite di età può essere abbassato dalla normativa nazione fino massimo ai 13 anni). Sotto tale età il consenso deve essere prestato da chi detiene la potestà genitoriale del minore

N.B. **il consenso raccolto prima del 25.05.2018 resta valido solo se ha tutte le caratteristiche previste dal nuovo regolamento.**

c) Interesse vitale di un terzo

Invocabile come base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione

f) Interesse legittimo prevalente di un titolare o di un terzo

- Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **non spetta** all'Autorità ma **è compito dello stesso titolare**

È una delle principali espressioni del **principio di «responsabilizzazione»** introdotto dal nuovo pacchetto protezione dati.

- L'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.

- Il regolamento chiarisce espressamente che l'interesse legittimo del titolar non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti

II. INFORMATIVA

Il regolamento indica in modo **tassativo** i contenuti dell'informativa (artt. 13 – 14) in parte più ampi rispetto al cod. privacy:

- Categoria di dati personali oggetto del trattamento
- Finalità del trattamento
- Dati di contatto del responsabile dei dati e del RPO (responsabile protezione dati) ove esistenti
- Base giuridica del trattamento
- Eventuale trasferimento dati a paesi terzi
- Periodo di conservazione dati
- Diritto dell'interessato
- Destinatari dei dati
- Processi decisionali automatizzati se posti in essere
- Ogni informazione necessaria a garantire un trattamento corretto e trasparente

- L’informativa deve essere effettuata **prima** della raccolta dei dati

N.B. il nuovo regolamento impone di specificare la finalità di trattamento dei dati ➡ ogni volta che le finalità cambiano occorre una nuova informativa all’interessato prima di procedere al trattamento

III. SOGGETTI

- **Titolare del trattamento**:

«*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 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*»

Viene prevista la **contitolarità del trattamento** *(art. 26)* che impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti, **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

Il regolamento introduce per la prima volta un obbligo di **valutazione di impatto sulla protezione dei dati** in capo ai titolari:

i Titolari dovranno effettuare una Valutazione degli impatti privacy (**Privacy Impact Assessment– PIA**) fin dal momento della progettazione del processo aziendale e degli applicativi informatici di supporto, nei casi in cui il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati.

Il PIA dovrà essere realizzato per trattamenti potenzialmente rischiosi attraverso l'analisi dei rischi, l'individuazione delle modalità tali di gestire correttamente i rischi, prevedendo dei controlli annuali sull'efficacia delle soluzioni adottate.

- **Responsabile del trattamento**:

«la persona fisica o giuridica, l'autorità pubblica o il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»

Il regolamento prevede degli obblighi specifici in capo al responsabile ove nominato (rimangono invariati i requisiti soggettivi e oggettivi già previsti nel cod. privacy):

- Tenuta del registro dei trattamenti svolti
- Adozione di misure tecniche e organizzative idonee a garantire la sicurezza dei trattamenti
- Eventuale designazione del Responsabile Protezione Dati

Secondo parte della dottrina con l'entrata in vigore del nuovo regolamento non sarà più possibile individuare un responsabile interno del trattamento

- Responsabile per la protezione dei dati (RPD) o Data Privacy Officer (DPO)

È una **nuova figura** introdotta dal Regolamento

Deve essere nominato dal titolare e dal responsabile del trattamento 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 responsabile della protezione dei dati è designato in funzione delle **qualità professionali**, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39».

Può essere un soggetto **interno o esterno alla struttura**

Compiti del DPO :

- 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 presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

IV. REGISTRO DEI TRATTAMENTI

- Il regolamento prevede l'elaborazione di un **sistema documentale di gestione delle privacy**, contenente tutti gli atti regolarmente aggiornati ed elaborati, al fine di soddisfare i requisiti di conformità al Regolamento.
- Il Titolare del trattamento dovrà dunque **conservare** la **documentazione di tutti i trattamenti effettuati** sotto la propria responsabilità, indicando obbligatoriamente, per ognuno di essi, una serie importante di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento (il Registro dei trattamenti potrà essere cartaceo ovvero multimediale).
- Tutte le operazioni di trattamento dovranno essere **tracciabili e documentabili**.

- La tenuta di un registro del trattamento è **obbligatoria** solo per le imprese od organizzazioni con più di 250 dipendenti.

- Le imprese od organizzazioni con meno di 250 dipendenti, invece, sono obbligate alla tenuta del Registro del trattamento solo nel caso in cui effettuino un trattamento in grado di presentare un **rischio per i diritti e le libertà dell'interessato** e, in **alternativa**:

- **non occasionale**;
- **relativo a categorie particolari di dati personali** ai sensi dell'art. 9.1 del Regolamento (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, 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)
- **relativo a condanne penali**, a reati o a connesse misure di sicurezza.

N.B. La tenuta di un registro del trattamento è in ogni caso **consigliabile** anche per le aziende con meno di 250 dipendenti:

il Regolamento, infatti, non esonera anche dall'obbligo di rendicontazione le aziende con meno di 250 dipendenti. In caso di controllo da parte dell'Autorità, il modo più sicuro per il titolare o il responsabile del trattamento di aver correttamente adempiuto ai dettami previsti dal Regolamento è quello di fornire evidenza cartacea per il tramite di un registro informatico (o di un documento equipollente).

V. VIOLAZIONE DEI DATI PERSONALI: OBBLIGHI DI SEGNALAZIONE

Per violazione dei dati personali (c.d. "**personal data breaches**") si intende: la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati.

I Titolari del trattamento, in caso di una violazione devono:

- Notificare la violazione all'Autorità di controllo entro 72 ore dal fatto
- Segnalare al diretto interessato (senza ritardo ingiustificato).

Il mancato rispetto di questo obbligo comporta sanzioni penali

La notifica all'Autorità:

- non è obbligatoria → è subordinata alla **valutazione del rischio per gli interessati**

che spetta al titolare del trattamento dei dati.

- Il Regolamento prevede quindi l'obbligo di notificare, entro le 72 ore e senza ingiustificato ritardo, soltanto in presenza di quelle violazioni che- secondo la valutazione del titolare- sono idonee a causare elevati rischi per i diritti e libertà degli interessati.
- Tutti i titolari del trattamento dovranno a tal fine documentare le violazioni dei dati subite, anche se non notificate all'Autorità di controllo e non comunicate agli interessati, nonchè le relative circostanze e i piani di miglioramento adottati.

Comunicazione all'interessato:

- Non è richiesta nei casi previsti dall'art. 34):

a) il titolare del trattamento ha messo in atto le **misure tecniche e organizzative adeguate di protezione** e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente **adottato misure atte a scongiurare il sopraggiungere di un rischio elevato** per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione **richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia

VI. NUOVI DIRITTI DELL'INTERESSATO

Il nuovo regolamento introduce inoltre dei **nuovi diritti in capo agli interessati**, ed in particolare:

Diritto all'oblio (right to be forgotten / right to erasure):

- si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) **di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati,** compresi "qualsiasi link, copia o riproduzione"
- Ha **un campo di applicazione più esteso** poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento

Diritto alla portabilità del dato (data portability):

- si intende il riconoscimento sia del diritto dell'interessato a **trasferire** i propri dati (es. quelli relativi al proprio "profilo utente") da un sistema di trattamento elettronico (es. Social Network) ad un altro senza che il Titolare possa impedirlo, sia del diritto di **ottenere gli stessi in un formato elettronico strutturato e di uso comune** che consenta di farne ulteriore uso.

VII. SANZIONI

il Regolamento UE ha innalzato sensibilmente la misura delle sanzioni, che potranno arrivare fino ad un massimo di **€ 20.000.000,00 o fino al 4% del fatturato annuo**.

Il Regolamento prevede altresì la possibilità per gli stati membri di prevedere ulteriori sanzioni, anche di carattere penale, che non siano in conflitto con le norme ed i principi disciplinati dalla nuova normativa europea.