STUDIO
LIVRAGHI
COMMERCIALISTI ASSOCIATI

Rag. Aurelio Livraghi
Rag. Commercialista – Tributarista – Revisore Legale

Dott. Alberto Livraghi
Dott. Commercialista – Revisore Legale

LA NUOVA DISCIPLINA SULLA PRIVACY PREVISTA DAL REGOLAMENTO UE 679/2016

Premessa

Con il regolamento UE 27.4.2016 n. 679 sono state introdotte alcune novità in materia di privacy.

Tale regolamento, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, è entrato in vigore il 24.5.2016, ma sarà applicabile dal prossimo 25.5.2018.

Mancano ancora le norme di coordinamento rispetto alla disciplina prevista dal vigente Codice della privacy (di cui al DLgs. 196/2003), che, quindi, alla data del **25.5.2018**, rimarrà in vigore, ma compatibilmente con il nuovo regolamento.

Alla data della presente circolare, risulta l'approvazione da parte del Consiglio dei Ministri, in esame preliminare, solo di uno schema di DLgs. recante le disposizioni per l'adeguamento della normativa nazionale al nuovo reg. UE 679/2016, in attuazione dell'art. 13 della L. 25.10.2017 n. 163 (legge di delegazione europea 2016-2017). Il suddetto DLgs., una volta emanato, sostituirà il vigente Codice della privacy e costituirà, insieme al regolamento europeo, la nuova disciplina in materia di privacy.

Oggetto e finalità del regolamento

Le disposizioni contenute nel reg. UE 679/2016 (art. 1 par. 1) riguardano la protezione delle persone fisiche (così come per il Codice della privacy, che esclude il trattamento dei dati relativi a persone giuridiche) con riferimento:

- al trattamento dei dati personali;
- alla libera circolazione di tali dati.

Ambito di applicazione materiale

Il reg. UE 679/2016 (art. 2) trova applicazione con riferimento ai seguenti trattamenti:

- trattamento automatizzato, in maniera parziale o totale, di dati personali;
- trattamento non automatizzato di dati personali contenuti in un archivio o destinati ad essere ivi inclusi.

Figure Professionali

Nell'ambito dei soggetti coinvolti nel trattamento dei dati personali, il reg. UE 679/2016 (Capo IV, artt. 24 - 43) continua a prevedere, rispetto al Codice della privacy (artt. 28 - 29), le figure del titolare del trattamento dei dati e del responsabile del trattamento dei dati.

Rag. Aurelio Livraghi
Rag. Commercialista – Tributarista – Revisore Legale
Dott. Alberto Livraghi
Dott. Commercialista – Revisore Legale

Il regolamento, poi, disciplina la nuova figura del responsabile per la protezione dei dati personali.

Titolare, responsabile e incaricato del trattamento dei dati

Il reg. UE 679/2016 definisce in maniera più precisa ruoli e compiti del titolare e del responsabile del trattamento dei dati. Tali qualifiche possono essere assunte da una persona fisica o giuridica, un'autorità pubblica, un servizio o altro organismo (art. 4 n. 7 e 8).

Responsabile del trattamento

Il responsabile del trattamento è il soggetto che tratta dati personali per conto del titolare del trattamento (art. 28 del reg. UE 679/2016).

Rispetto al Codice della privacy:

- viene prevista una più specifica definizione dei rapporti fra titolare e responsabile, che deve avvenire mediante il ricorso a un contratto (o altro atto giuridico), in forma scritta (anche in formato elettronico), con uno specifico contenuto;
- il responsabile del trattamento può ricorrere ad un altro responsabile solo su autorizzazione scritta (specifica o generale) del titolare del trattamento;
- può essere nominato un sub-responsabile del trattamento, per specifiche attività di trattamento, nel qual caso occorre definire i rapporti mediante un contratto o altro atto giuridico.

La violazione del regolamento da parte del responsabile del trattamento, determinando finalità e mezzi del trattamento stesso, comporta l'assunzione diretta della qualifica di titolare del trattamento.

Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate onde assicurare la conformità del trattamento al regolamento e alla tutela dei diritti dell'interessato (dimostrata anche mediante il ricorso a Codici di condotta o meccanismi di certificazione).

Responsabile della protezione dei dati

Il reg. UE 679/2016 (artt. 37 - 39) introduce la nuova figura professionale del responsabile della protezione dei dati - RPD (o Data Protection Officer - DPO), di cui si forniscono le principali caratteristiche nella seguente tabella.

STUDIO
LIVRAGHI
COMMERCIALISTI ASSOCIATI

Rag. Aurelio Livraghi
Rag. Commercialista – Tributarista – Revisore Legale

Dott. Alberto Livraghi
Dott. Commercialista – Revisore Legale

Nomina	La nomina dell'RPD è obbligatoria per: • l'autorità pubblica o l'organismo pubblico (salvo il trattamento dei dati sia effettuato dalle autorità giurisdizionali nell'esercizio delle funzioni giurisdizionali); • tutti i soggetti la cui attività principale consista in trattamenti che, per la loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; • tutti i soggetti la cui attività principale consista nel trattamento, su larga scala, di categorie particolari di dati personali (nell'ambito dei quali sono compresi i dati definiti dal Codice della privacy come "sensibili", oltre ai nuovi dati genetici e biometrici) e i dati relativi a condanne penali e reati (artt. 9 e 10 del reg. UE 679/2016).
Qualifica e designazione	L'RPD viene designato dal titolare del trattamento e dal responsabile del trattamento: • in funzione delle qualità professionali (conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati) e della capacità di assolvere i propri compiti; non sono necessarie attestazioni formali o titoli professionali specifici; • ricorrendo a un proprio dipendente (RPD interno) o a un soggetto esterno (RPD esterno), in quest'ultimo caso mediante il ricorso ad un contratto di servizi. È possibile per un gruppo di imprese o di soggetti pubblici nominare un unico RPD.
Compiti	L'RPD deve svolgere i seguenti compiti minimi: • informare e fornire consulenza al titolare o al responsabile del trattamento, nonché ai dipendenti, in merito agli obblighi derivanti dal regolamento; • verificare l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi auditors; • fornire, se richiesto, pareri in merito alla valutazione di impatto sulla protezione dei dati e sorvegliare i relativi adempimenti; • fungere da punto di contatto con l'autorità di controllo o, eventualmente, consultarla di propria iniziativa. Nell'esecuzione di tali compiti, l'RPD: • deve essere "sostenuto", mediante il rilascio delle risorse necessarie; • non deve ricevere alcuna istruzione; • non è rimosso o penalizzato.

Rag. Aurelio Livraghi
Rag. Commercialista – Tributarista – Revisore Legale
Dott. Alberto Livraghi
Dott. Commercialista – Revisore Legale

Obblighi	È tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti (che possono essere anche altri, purché non integrino un conflitto di interessi).
Adempimenti	I dati di contatto del responsabile della protezione dei dati devono essere pubblicati e comunicati all'autorità di controllo da parte del titolare del trattamento e dal responsabile del trattamento.

Adempimenti del titolare del trattamento e del responsabile del trattamento

In capo al titolare del trattamento e al responsabile del trattamento sono stati:

- dettagliati e/o modificati alcuni adempimenti già previsti dal Codice della privacy, ad esempio in materia di modalità di trattamento dei dati, di acquisizione del consenso e di rilascio dell'informativa;

- introdotti nuovi compiti, fra i quali tenere un registro delle attività di trattamento ed effettuare una valutazione di impatto sulla protezione dei dati.

Modalità di trattamento dei dati

Il titolare del trattamento deve previamente istruire tutti coloro che siano autorizzati ad accedere e trattare i dati personali, compreso il responsabile del trattamento (art. 29 del reg. UE 679/2016).

Costituiscono principi generali del trattamento (art. 5 del reg. UE 679/2016):

- la liceità, la correttezza e la trasparenza nei confronti dell'interessato;
- la limitazione delle finalità (determinate, esplicite e legittime);
- la minimizzazione dei dati, che devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- l'esattezza, con aggiornamento dei dati se necessario;
- la limitazione della conservazione;
- l'integrità e la riservatezza;
- la responsabilizzazione del titolare del trattamento, il quale è competente per il rispetto dei principi sopra esposti e sul quale grava l'onore di prova.

Con specifico riguardo alla liceità del trattamento, il regolamento conferma che questo deve trovare fondamento su un'idonea base giuridica, che corrisponde in linea di massima a quella del vigente Codice della privacy (artt. 11 e 23).

STUDIO
LIVRAGHI
COMMERCIALISTI ASSOCIATI

Rag. Aurelio Livraghi
Rag. Commercialista – Tributarista – Revisore Legale
Dott. Alberto Livraghi
Dott. Commercialista – Revisore Legale

Il trattamento è lecito se ricorrono i seguenti presupposti (art. 6 del reg. UE 679/2016):

consenso dell'interessato per una o più specifiche finalità;

adempimento di obblighi contrattuali, di cui l'interessato è parte o di misure precontrattuali;

obblighi di legge cui è soggetto il titolare del trattamento;

interessi vitali della persona interessata o di terzi;

interesse pubblico o esercizio di pubblici poteri;

interesse legittimo del titolare del trattamento o di terzi cui i dati vengono comunicati, la cui prevalenza – rispetto al Codice della privacy – è valutata dallo stesso titolare del trattamento (per effetto del principio di responsabilizzazione).

Acquisizione del consenso

Come già previsto dal Codice della privacy (art. 23), il consenso deve essere libero, specifico rispetto alle finalità del trattamento (o per finalità compatibili), informato.

Rispetto però al Codice della privacy, che stabilisce espressamente la forma scritta per la prova del consenso al trattamento dei dati in generale e per la stessa validità in caso di dati sensibili, il regolamento non precisa le modalità di espressione del consenso.

Il regolamento richiede il consenso "esplicito" solo per:

- categorie particolari di dati;
- le decisioni basate su trattamenti automatizzati (compresa la profilazione).

La richiesta di consenso, qualora inserita all'interno di una dichiarazione scritta, deve essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato e deve essere resa in forma comprensibile e facilmente accessibile, con linguaggio semplice e chiaro.

Il consenso dei minori è valido a partire dai 16 anni, mentre prima occorre il consenso dei genitori o di chi ne fa le veci.

Categorie particolari di dati personali

Sono inclusi nella nuova definizione di "categorie particolari di dati" quelli attualmente previsti dal Codice della privacy come dati "sensibili", quindi i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oltre ai dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 del reg. UE 679/2016 e art. 4 co. 1 lett. d) del Codice della privacy).

STUDIO
LIVRAGHI
COMMERCIALISTI ASSOCIATI

Rag. Aurelio Livraghi
Rag. Commercialista – Tributarista – Revisore Legale
Dott. Alberto Livraghi
Dott. Commercialista – Revisore Legale

Informativa

Il reg. UE 679/2016 (artt. 13 e 14) riprende, rispetto al Codice della privacy (art. 13), l'obbligo di informativa, distinto sempre rispetto alla raccolta dei dati presso l'interessato o meno, prevedendo però un contenuto maggiormente dettagliato.

L'informativa deve:

- avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile e deve essere utilizzato un linguaggio chiaro e semplice;
- essere data per iscritto o con "altri mezzi" anche elettronici (ad esempio, nel caso di servizi on line), oralmente se richiesto dall'interessato (il Codice della privacy prevede solo in forma scritta od orale); è ammesso l'uso di icone.

Diritti degli interessati

Nell'ambito dei diritti previsti in capo all'interessato, vengono ripresi, rispetto al Codice della privacy, oltre all'informativa sul trattamento dei dati personali, i seguenti (artt. 12 - 23 del reg. UE 679/2016):

- diritto di accesso;
- diritto di rettifica;
- diritto di cancellazione (diritto all'oblio in forma rafforzata);
- diritto di opposizione.

Viene previsto, poi, il diritto alla limitazione al trattamento dei dati, che costituisce un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui al Codice della privacy (art. 7 co. 3 lett. b)).

Viene introdotto, infine, il nuovo diritto alla portabilità dei dati, che riguarda i trattamenti:

basati sul consenso o su un contratto stipulato con l'interessato;

effettuati con mezzi automatizzati.

Inoltre, si deve trattare di dati forniti direttamente dall'interessato al titolare del trattamento.

Principio di "accountability"

Viene introdotto il principio della c.d. "responsabilizzazione" (accountability) di titolari (e responsabili) del trattamento, che sono tenuti a mettere in atto misure tecniche e organizzative adeguate per garantire e per dimostrare l'applicazione del regolamento, con gli aggiornamenti necessari (art. 24 del reg. UE 679/2016).

Rag. Aurelio Livraghi
Rag. Commercialista – Tributarista – Revisore Legale
Dott. Alberto Livraghi
Dott. Commercialista – Revisore Legale

Pertanto, è il titolare che decide in maniera autonoma modalità, garanzie e limiti del trattamento dei dati personali, nel rispetto del regolamento e di alcuni criteri previsti (ad esempio, fra questi vi è il principio della privacy "by design" e "by default").

Principio della privacy "by design" e "by default"

Viene richiesto al titolare del trattamento di impostare da subito l'attività e la stessa organizzazione secondo i principi c.d. di "privacy by design" e "privacy by default", riducendo i trattamenti non necessari (art. 25 del reg. UE 679/2016).

In particolare:

"privacy by design": occorre attuare adeguate misure tecniche e organizzative sin dall'atto della progettazione (quindi, prima di procedere al trattamento dei dati) e comunque al momento dell'esecuzione del trattamento; fra le misure vengono indicate espressamente la pseudonimizzazione e la minimizzazione;

"privacy by default": i dati vengano trattati, per impostazione predefinita, esclusivamente per le finalità previste e per il periodo strettamente necessario (in maniera similare a quanto già previsto dal Codice della privacy con il principio di necessità); le misure devono garantire che i dati personali non siano resi accessibili a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

La conformità ai requisiti richiesti può essere dimostrata mediante il ricorso a meccanismi di certificazione.

Registro delle attività di trattamento

I titolari e i responsabili del trattamento devono tenere un registro delle operazioni di trattamento, in forma scritta, anche in formato elettronico (art. 30 del reg. UE 679/2016).

Sono escluse da tale obbligo le imprese o le organizzazioni con meno di 250 dipendenti, salvo che il trattamento:

- possa presentare un rischio per i diritti e le libertà dell'interessato;
- non sia occasionale;
- includa il trattamento di categorie particolari di dati o di dati personali relativi a condanne penali e a reati.

Sanzioni

Il Regolamento individua due categorie di sanzioni amministrative a seconda della natura della violazione.

1. e' prevista la sanzione amministrativa pecuniaria fino a 10 milioni di euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (ad esempio nel caso di violazioni riguardanti attività di trattamento e nomina del Responsabile della protezione dei dati personali)

STUDIO
LIVRAGHI
COMMERCIALISTI ASSOCIATI

Rag. Aurelio Livraghi
Rag. Commercialista – Tributarista – Revisore Legale

Dott. Alberto Livraghi
Dott. Commercialista – Revisore Legale

2. fino a 20 milioni di euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (ad esempio nel caso di violazione dei diritti degli interessati)

Vi invitiamo a contattare il Vostro consulente in materia di privacy nel caso non ne aveste uno il nostro studio ha preso contatti con esperti del settore e si rende disponibile a fornirvi tutti i riferimenti.

Lo studio rimane a disposizione per ogni ulteriore chiarimento.

Distinti saluti.

Dott. Alberto Livraghi