Circolare n. 41 FR/cg 4 luglio 2017

PRIVACY – NUOVO REGOLAMENTO UE 2016/679

Con il Reg. UE n. 679/2016 (di cui si allega copia) il Parlamento Europeo ed il Consiglio dell'Unione Europea hanno approvato una nuova disciplina in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali ed alla libera circolazione di tali dati.

Il regolamento è entrato in vigore il 24 maggio 2016 ma **si applica a decorrere dal 25 maggio 2018**, termine quest'ultimo dal quale è abrogata la direttiva 95/46/CE.

Pertanto, si precisa che fino al **25 maggio 2018** si applicano le disposizioni del D.Lgs. n. 196/2003 (cd. Codice della privacy).

Il regolamento, inoltre, attribuisce alla Commissione europea il potere di adottare atti delegati e di esecuzione e agli Stati la facoltà di disciplinare determinati ambiti individuati dal regolamento stesso.

E' opportuno, di seguito, evidenziare per gli aspetti competenza le principali novità introdotte col Regolamento in esame.

Ambito di applicazione (artt. 2-3)

Il regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Con riguardo, invece, all'ambito di applicazione territoriale, il regolamento si applica:

- al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione;
- al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
  a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
  b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Liceità del trattamento (art. 6)

L'art. 6 del regolamento stabilisce che il trattamento dei dati personali è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali

dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

In buona sostanza il Regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica le cui condizioni di liceità sono quelle sopra elencate.

Sempre nell'articolo 6 viene anche previsto che, nel caso in cui il trattamento non fosse compatibile con le finalità per le quali i dati personali erano stati raccolti, il titolare del trattamento è tenuto a verificare che la diversa finalità cui è soggetto il trattamento sia comunque compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti.

Consenso (art. 7)

Giova evidenziare che, ai sensi dell'art. 6 del regolamento, il consenso[1] è una delle condizioni di liceità del trattamento di dati personali, a differenza del D.Lgs. n. 196/2003 che lo considera quale condizione generale di ammissibilità del trattamento (salvo i casi in cui può essere fatto un trattamento senza consenso).

L'art. 4, comma 1, n. 11 del regolamento definisce il consenso dell'interessato come 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 personal**i che lo riguardano siano oggetto di trattamento.

In particolare, si rileva che il considerando 32 del provvedimento prevede che "*il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale*".

Si precisa, dunque, che il regolamento non impone la forma scritta come condizione obbligatoria per il rilascio del consenso, ma stabilisce espressamente all'art. 7 che, qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Per i dati sensibili (si veda art. 9 regolamento) il consenso **deve** essere "e-

[1] L'articolo 8, paragrafo 1, del Regolamento prevede, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, che il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. 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 dal titolare della responsabilità genitoriale.

splicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione art. 22).

Sempre l'articolo 7 precisa che se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, **la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie**, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro (tra l'altro è precisato che nessuna parte di una tale dichiarazione che costituisca una violazione del regolamento è vincolante).

Infine, viene puntualizzato che nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Dati sensibili (artt. 9-10)

L'art. 9 del regolamento sancisce **il divieto di trattamento di dati personali che rivelino** l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché di 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, **salvo che in determinati casi**.

Tra i casi di deroga al divieto di trattamento, elencati al comma 2 dell'art. 9, rientra l'ipotesi in cui l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche.

L'attuale Codice della Privacy, invece, stabilisce che i dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante (salvo determinati casi di deroga).

L'articolo 10 prevede che il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'Autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (art. 12)

Si evidenzia che, ai sensi dell'art. 12 del regolamento, il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

La norma citata precisa che le informazioni sono fornite **per iscritto o con altri mezzi**, anche, se del caso, con mezzi elettronici; tuttavia, se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Sempre l'art. 12, inoltre, prevede che l'informativa può essere fornita **in combinazione** con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto.

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato o non siano stati ottenuti presso l'interessato (art. 13-14)

Gli articoli 13 e 14 prevedono i contenuti tassativi dell'informativa che devono essere indicati a seconda che i dati siano o meno raccolti presso l'interessato (negli stessi articoli sono anche previsti i casi di esonero dell'informativa).

Per la disamina completa delle informazioni che devono essere fornite si rinvia al testo degli articoli, tuttavia si segnala già in questa sede che – oltre alle informazioni, ad esempio, relative all'identità ed ai dati del titolare, ai dati di contatto del responsabile della protezione dei dati, ove applicabile – sono previste altre informazioni, tra cui: il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; la base giuridica del trattamento; qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento; se ha intenzione di trasferire i dati personali in Paesi terzi; l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Per quanto riguarda la tempistica dell'informativa si evidenzia che nel caso in cui i dati personali sono raccolti presso l'interessato le informazioni sono fornite nel momento in cui i dati personali sono ottenuti.

Qualora invece i dati non sono raccolti presso l'interessato, il titolare del trattamento fornisce le informazioni:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma **al più tardi entro un mese**, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Diritto di accesso dell'interessato (art. 15)

L'art. 15 del regolamento prevede che, in caso di esercizio del diritto di accesso[2], l'interessato deve essere informato (e ricevere una copia dei dati personali trattati) in ordine ad una serie di informazioni, alcune delle quali non sono attualmente contemplate nel Codice della privacy, quali ad esempio:

- il periodo di conservazione dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- il diritto di proporre reclamo dinanzi all'Autorità di controllo;
- sulla origine dei dati personali qualora gli stessi non siano raccolti

[2] Il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano.

direttamente presso l'interessato;
- l'eventuale esistenza di un processo decisionale automatizzato, tra cui la profilazione.

Diritto alla cancellazione cd "diritto all'oblio" (art. 17)

L'art. 17 del regolamento stabilisce espressamente una serie di ipotesi nelle quali l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali (diritto all'oblio) che lo riguardano senza ingiustificato ritardo.

Il diritto di oblio con il Regolamento viene rafforzato prevedendo espressamente i motivi che legittimano il diritto dell'interessato ad ottenere la cancellazione dei dati e precisamente:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8 paragrafo 1 del Regolamento.

Il comma 2 dell'art. 17 citato, inoltre, prevede in caso di cancellazione che il titolare del trattamento, se ha reso pubblici dati personali, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Diritto di limitazione (art. 18)

L'articolo in commento prevede un diritto **diverso e più esteso rispetto al "blocco" del trattamento** di cui all'art. 7, comma 3, lettera b), del Codice, in particolare, è esercitabile da parte dell'interessato **non solo in caso di violazione** dei presupposti di liceità del trattamento, bensì anche **se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare**) o **si oppone al loro trattamento** ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

E' opportuno precisare che il considerando 67 del Regolamento specifica che "*le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe*

indicare chiaramente che il trattamento dei dati personali è stato limitato".

Diritto di opposizione (art. 21)

L'art. 21 del regolamento disciplina il diritto dell'interessato di opporsi al trattamento dei dati personali che lo riguardano effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri o per il perseguimento del legittimo interesse del titolare del trattamento o di terzi a cui i dati vengono comunicati, compresa la profilazione.

Qualora i dati personali siano trattati per **finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità,** compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Diritto alla portabilità dei dati (art. 20)

L'art. 20 del regolamento introduce il diritto alla portabilità dei dati, ovvero il diritto dell'interessato di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.

Al riguardo, si precisa che tale nuovo diritto[3] potrà essere esercitato a condizione che il trattamento si basi sul consenso o su un contratto e il trattamento sia effettuato con mezzi automatizzati.

Giova evidenziare, inoltre, che nell'esercizio del diritto alla portabilità dei dati **l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro,** se tecnicamente fattibile.

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (art. 22)

L'art. 22 del regolamento stabilisce che l'interessato ha il diritto di non essere sottoposto a 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.

A tal riguardo, il medesimo articolo prevede e disciplina deroghe all'applicazione del suddetto diritto e precisamente nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato ed un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è

[3] Il Gruppo "Articolo 29" (organismo consultivo e indipendente composto da un rappresentante delle Autorità di protezione dati designato da ciascun stato membro) ha pubblicato delle linee-guida specifiche dove sono illustrati e spiegati i requisiti e le caratteristiche del diritto alla portabilità con particolare riguardo ai diritti di terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi all'interessato" di cui quest'ultimo chiede la portabilità con le relative FAQ. La versione italiana è disponibile sul sito del Garante: **http://www.garanteprivacy.it/** con le relative FAQ.

soggetto il titolare;
- si basi sul consenso esplicito dell'interessato.

Titolare e responsabile del trattamento (artt. 24-31)

Il regolamento prevede che, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve mettere in atto **misure tecniche e organizzative adeguate** per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.

In tale ottica, l'art. 25 del regolamento stabilisce che **sia al momento** di determinare i mezzi del trattamento **sia all'atto del trattamento** stesso il titolare del trattamento deve mettere 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 regolamento e tutelare i diritti degli interessati (cd. *privacy by design*).

Sempre l'art. 25 citato, inoltre, obbliga il titolare del trattamento a mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento, specificando che tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità (cd. *privacy by default*).

In particolare, viene previsto che dette misure devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Con riferimento al responsabile del trattamento (ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare), invece, l'art. 28 del regolamento disciplina gli obblighi ed il rapporto con il titolare del trattamento, **che devono essere regolati e specificati da un contratto o da altro atto giuridico** (in forma scritta, anche in formato elettronico) a norma del diritto dell'Unione o degli Stati membri.

In particolare, il contratto deve vincolare il responsabile del trattamento al titolare del trattamento e regolare la materia disciplinata, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Sempre gli articoli in esame prevedono che il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche (il responsabile del trattamento che ha nominato sub responsabili risponde innanzi al titolare dell'inadempimento dell'eventuale sub-responsabile).

Giova, inoltre, evidenziare che l'art. 30 del regolamento prevede l'obbligo

per il titolare ed il responsabile di trattamento (e ove applicabile i loro rappresentanti ai sensi dell'art. 27) di tenere un **registro delle attività di trattamento in forma scritta**, anche in formato elettronico.

Al riguardo, relativamente al titolare del trattamento (e ove applicabile il suo rappresentante) viene stabilito che il registro deve contenere le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Con riguardo al responsabile del trattamento (e, ove applicabile, il suo rappresentante), invece, l'art. 30 prevede che il registro contenga tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, includendo le seguenti informazioni:

- il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- ove applicabile, i trasferimenti di dati verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie adeguate;
- ove possibile, una descrizione generale delle misure tecniche e organizzative di cui all'articolo 32, paragrafo 1.

L'art. 30 citato, tuttavia, precisa che l'obbligo del registro per titolare e responsabile di trattamento **non si applica alle imprese o organizzazioni con meno di 250 dipendenti**, **a meno che il trattamento che esse effettuano 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 (sensibili) o i dati personali relativi a condanne penali e a reati**.

Sicurezza dei dati personali (artt. 32-34)

L'art. 32 del regolamento sancisce il dovere del titolare e del responsabile del trattamento di **mettere in atto misure tecniche e organizzative adeguate** a garantire un livello di sicurezza adeguato al rischio derivante dal trattamento per i diritti e le libertà delle persone fisiche (tra le quali ad esempio sono ricomprese anche la pseudonimizzazione e la cifratura dei dati personali).

In tale ottica, l'art. 33 del regolamento prevede che, in caso di violazione dei dati personali, il titolare del trattamento **deve notificare la violazione** all'autorità di controllo competente **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[4].

Il regolamento, inoltre, dispone all'art. 34 che, 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 deve comunicare la violazione all'interessato senza ingiustificato ritardo.

Tale comunicazione all'interessato, tuttavia, non è richiesta in presenza delle condizioni previste dall'art. 34 citato, tra le quali rientrano l'applicazione ai dati personali oggetto di violazione di misure adeguate di protezione (quali la cifratura), l'adozione di misure successive alla violazione atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati ovvero la natura sproporzionata dello sforzo per effettuare la comunicazione (in tal caso si può procedere anche a una comunicazione pubblica).

Valutazione d'impatto sulla protezione dei dati personali (artt. 35-36)

L'art. 35 del regolamento stabilisce che, quando un tipo di trattamento (allorchè prevede in particolare l'uso di nuove tecnologie e considerati la natura, oggetto e finalità) può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, **effettua una valutazione dell'impatto** dei trattamenti previsti sulla protezione dei dati personali.

A tal riguardo, viene espressamente previsto che la valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali (sensibili) o di dati relativi a condanne penali e a reati;
- la sorveglianza sistematica su larga scala di una zona accessibile al

[4] Si ricorda che l'Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico (si veda, **http://www.garanteprivacy.it/** che intende, secondo quanto indicato nella Guida all'applicazione del regolamento, rielaborare al fine di renderlo utilizzabile da tutti i titolari di trattamento secondo quanto prevede il regolamento).

pubblico.

In tale ottica, l'art. 35 citato prevede che l'autorità di controllo redige un elenco delle tipologie di trattamenti per cui è richiesta una valutazione d'impatto e può anche redigere un elenco per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati.

L'art. 36 del regolamento, inoltre, sancisce l'obbligo per il titolare del trattamento di consultare l'autorità di controllo, prima di procedere al trattamento, qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

In tal caso viene stabilito che l'autorità di controllo fornisce un parere scritto al titolare del trattamento, se ritiene che il trattamento previsto violi il regolamento (in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio).

Responsabile della protezione dei dati (artt. 37-39)

L'art. 37 del regolamento dispone l'obbligo per il titolare e il responsabile del trattamento di designare un responsabile della protezione dei dati (Data Protection Officer – DPO)[5] 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** (sensibili) o **di dati relativi a condanne penali e a reati**.

Il regolamento prevede in particolare che 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 previsti;
- può essere un dipendente del titolare o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi;
- deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali dal titolare e dal responsabile del trattamento;
- è sostenuto nell'esecuzione dei suoi compiti dal titolare e dal responsabile del trattamento, che devono fornirgli le risorse necessa-

[5] Il WP29 ha ritenuto opportuno fornire alcune linee-guida di recente pubblicazione sulla figura del DPO, disponibili anche sul sito del Garante, e alle quali si rinvia per maggiori delucidazioni unitamente alle relative FAQ (si veda: **http://www.garanteprivacy.it/**).

rie per assolvere tali compiti e per mantenere la propria conoscenza specialistica;
- non riceve alcuna istruzione per l'esecuzione delle sue funzioni, non può essere a tal fine rimosso o penalizzato per l'adempimento dei suoi compiti,
- riferisce direttamente al vertice gerarchico del titolare o del responsabile del trattamento;
- è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti;
- è il punto di contatto per gli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

Con riguardo ai suoi compiti, l'art. 39 del regolamento stabilisce che il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare 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;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Codici di condotta e certificazione (artt. 40-43)

L'art. 40 del regolamento disciplina i codici di condotta, che le associazioni e gli altri organismi rappresentanti le categorie di titolari o responsabili del trattamento possono elaborare allo scopo di precisare l'applicazione del regolamento.

In particolare, viene previsto che i codici devono essere sottoposti al parere dell'autorità di controllo che ne certifica la conformità con il regolamento e che la Commissione europea può attribuirgli validità generale all'interno dell'Unione europea.

L'art. 42 del regolamento, invece, consente un procedimento di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al regolamento dei trattamenti effettuati dai titolari e dai responsabili del trattamento.

Mezzi di ricorso, responsabilità e sanzioni (artt. 77-84)

Il regolamento prevede una serie di mezzi di ricorso che l'interessato ha a disposizione qualora ritenga che il trattamento che lo riguarda violi il rego-

lamento stesso. In particolare l'interessato può proporre:

- un reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione;
- un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che riguarda l'interessato;
- oppure qualora l'autorità di controllo competente non tratti un reclamo o non informi l'interessato entro tre mesi dello stato o dell'esito del reclamo proposto;
- un ricorso giurisdizionale effettivo nei confronti del titolare o del responsabile del trattamento dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare o il responsabile del trattamento ha uno stabilimento oppure in cui l'interessato risiede abitualmente.

Il regolamento, inoltre, stabilisce che chiunque subisca un danno materiale o immateriale causato da una violazione del regolamento stesso ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento.

A tal riguardo, viene previsto che il titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento e che il responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento (salvo che il titolare o il responsabile del trattamento dimostri che l'evento dannoso non gli è in alcun modo imputabile).

Al fine di garantire il risarcimento effettivo dell'interessato viene previsto che, qualora più titolari del trattamento o responsabili del trattamento oppure entrambi (il titolare del trattamento e il responsabile del trattamento) siano coinvolti nello stesso trattamento e responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno.

Con riguardo, invece, alle **sanzioni**, l'art. 83 del regolamento stabilisce che ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie siano in ogni singolo caso effettive, proporzionate e dissuasive nonché comminate tenendo in considerazione una serie di criteri tra cui, ad esempio, la natura, la gravità e la durata della violazione, il carattere doloso o colposo della violazione, le misure adottate dal titolare o dal responsabile del trattamento per attenuare il danno.

In particolare, è prevista la sanzioni amministrative pecuniarie **fino a 10.000.000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale** annuo dell'esercizio precedente, se superiore, per le violazioni delle seguenti disposizioni del regolamento riguardanti:

a) gli obblighi del titolare e del responsabile del trattamento;
b) gli obblighi dell'organismo di certificazione;
c) gli obblighi dell'organismo che controlla la conformità del codice di condotta;

Sempre l'articolo 83 prevede la sanzioni amministrative pecuniarie **fino a**

20.000.000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni delle seguenti disposizioni del regolamento riguardanti:

a) i principi di base del trattamento, comprese le condizioni relative al consenso;
b) i diritti degli interessati;
c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate per disposizioni relative a specifiche situazioni di trattamento;
e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo o il negato accesso in violazione all'articolo 58.

E', inoltre, previsto che l'inosservanza di un ordine impartito da parte dell'autorità di controllo nell'esercizio dei poteri correttivi previsti dall'art. 58, parag. 2, è **soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore**.

Ai sensi dell'art. 84 del regolamento, infine gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del regolamento in particolare per le violazioni non soggette alle sanzioni amministrative pecuniarie di cui all'art. 83 sopra citato.


allegato