La tutela della privacy

L'impresa che svolge un'attività di e-commerce si troverà necessariamente a svolgere delle operazioni di **trattamento di dati personali** oggetto di tutela attualmente ai sensi del **D.lgs. 196/2003, Codice in materia di protezione dei dati personali (Codice della privacy)** e, a partire dal **25 maggio 2018**, del **Regolamento UE 2016/679** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Dato che ci troviamo in un periodo di transizione, riteniamo necessario trattare innanzitutto della disciplina tutt'ora vigente, per poi passare all'esame delle novità introdotte dal Regolamento sui temi di rilievo per chi svolge attività di e-commerce.

Per determinare l'ambito di applicazione della suddetta normativa è bene chiarire che per **dato personale** si intende qualunque informazione relativa a un soggetto (solo **persone fisiche** a seguito della semplificazione introdotta dalla Legge 214/2011) che lo identifichi direttamente (esempio nome e cognome) o che lo renda anche solo indirettamente identificabile mediante un "ragionevole sforzo", ad esempio la partita Iva (art. 4. c. 1 lett. b Codice della privacy). Al contrario, quindi, non sono dati personali i dati anonimi, ossia i dati che non consentano l'identificazione della persona cui si riferiscono nemmeno tramite un ragionevole sforzo. Alcuni specifici dati personali sono definiti dalla legge "dati personali sensibili" e altri "dati personali giudiziari"; tutti gli altri dati personali si definiscono normalmente "dati personali comuni".

Come sopra detto, a partire dal 2012, le norme in tema di tutela della privacy si applicano solo nei confronti delle persone fisiche e non più nei confronti degli altri soggetti di diritto, quali ad esempio le società. Si consideri tuttavia che, nella maggior parte dei casi, le imprese che effettuano attività di e-commerce si trovano a dover trattare, allo stesso tempo e con i medesimi strumenti, dati personali relativi a persone fisiche e ad altri soggetti di diritto: ciò accade quando si svolgano contestualmente attività di B2B e di B2C, ma anche nell'ambito del solo B2B, dato che, nella pratica, non si distinguono i clienti tra imprese individuali e imprese costituite in forma societaria, il che accade anche sul fronte dei fornitori, sia nel B2B sia nel B2C.

Quali sono i trattamenti di dati personali che rilevano al fine dell'applicazione della suddetta normativa? Per "**trattamento**" si intende **qualunque operazione** o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici: a partire della **raccolta e registrazione dei dati personali**, la loro organizzazione, anche solo la mera **conservazione o consultazione** dei dati personali, la loro **elaborazione**, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e la distruzione di dati personali, anche se non registrati in una banca dati (art. 4, c. 1, lett. a). Per "comunicazione" si intende la rivelazione del dato a soggetti determinati e per "diffusione" la rivelazione del dato a soggetti indeterminati (ad esempio a mezzo stampa o Internet). Inoltre per "blocco" si intende la sospensione di ogni trattamento, ad eccezione

della conservazione del dato. Il blocco può essere disposto dal Garante per trattamenti in violazione di legge, inclusa la mancata adozione di misure di sicurezza.

I protagonisti della normativa in tema di tutela della privacy sono:

- l'**interessato**, la persona fisica cui si riferiscono i dati personali (art. 4, c. 1, lett. i), ossia nel caso dell'e-commerce i clienti (consumatori e ditte individuali) attuali e potenziali (ossia i soggetti nei confronti dei quali si svolgono attività promozionali), i fornitori (ditte individuali), i dipendenti e altri collaboratori dell'impresa, i consulenti e le altre persone fisiche di cui il titolare tratta dati personali
- il **titolare**, il soggetto cui competono le decisioni relative alle finalità e alle modalità del trattamento di dati personali nonché gli strumenti utilizzati (art. 4, c. 1, lett. f), ossia nel nostro caso l'impresa che effettua l'attività di *e-commerce*
- i **responsabili**, i soggetti (persone fisiche, società o altri enti), anche esterni rispetto al titolare, preposti dal titolare al trattamento di dati personali (art. 4, c. 1, lett. g)
- gli **incaricati**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile (art. 4, c. 1, lett. h). Si tratta dei dipendenti dell'impresa, dei collaboratori, di consulenti e fornitori incaricati dall'impresa di svolgere, specifiche operazioni di trattamento di dati personali.

È opportuno che l'impresa titolare informi, possibilmente per iscritto, i soggetti che svolgono attività di trattamento di dati personali per suo conto, quali responsabili e incaricati, interni ed esterni, delle regole da osservare e degli adempimenti da espletare. Per quanto attiene ai soggetti esterni, queste regole e relative responsabilità, sono di solito oggetto di specifici contratti, mentre per quanto riguarda il personale interno è opportuno organizzare degli interventi formativi.

I dati personali devono venire trattati nel rispetto dei **principi legislativi** che regolano tutti i trattamenti di dati personali. Gli strumenti informatici dell'impresa devono quindi essere improntati al rispetto dei principi di seguito illustrati, così come qualsiasi altra operazione di trattamento di dati personali effettuata dall'impresa con mezzi diversi:

- **principio di liceità e correttezza**. I dati personali devono essere trattati in modo lecito e secondo correttezza (art. 11, c. 1, lett. a)
- **principio di necessità**. Il trattamento di dati personali deve essere ridotto al minimo ed escluso in tutti i casi in cui le finalità perseguite possano essere realizzate per mezzo di dati anonimi o di dati "anonimizzati" mediante modalità che permettano di identificare l'interessato solo in caso di necessità (art. 11, c. 1, lett. e)
- **principi di finalità, pertinenza e non eccedenza**. I dati personali devono essere raccolti e registrati per scopi legittimi, determinati ed esplicitati all'interessato al momento della raccolta e devono essere utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi (art. 11, c. 1, lett. b). I dati personali trattati devono quindi essere pertinenti in relazione alle finalità per le quali sono raccolti e non eccedenti:

- né sotto il profilo sostanziale, non si devono raccogliere e trattare dati in più rispetto a quanto necessario in considerazione delle finalità perseguite e indicate all'interessato al momento della raccolta (art. 11, c. 1, lett. d)
- né sotto il profilo temporale, i dati personali devono essere trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente conservati in una forma che non consenta l'identificazione dell'interessato (art. 11, c. 1, lett. e).

I database dell'impresa devono quindi essere strutturati per garantire il rispetto di questi principi, non consentendo, ad esempio, il "caricamento" di dati non pertinenti o eccedenti e prevedendo sistemi di archiviazione dei dati divenuti eccedenti sotto il profilo temporale (ad esempio con automatismi periodici, la cui cadenza dipende dall'attività svolta)

- **principi di completezza, esattezza e aggiornamento**. La completezza, esattezza e l'aggiornamento dei dati personali devono essere curate sia al momento della raccolta e registrazione sia nelle fasi successive di trattamento (art. 11, c. 1, lett. c e lett. d). I database dell'impresa devono quindi essere strutturati per garantire il rispetto di questi principi, non consentendo, ad esempio, il "caricamento" di dati incompleti.

Per quanto attiene alle procedure, il primo essenziale adempimento **obbligatorio per qualsiasi trattamento di dati personali** è rappresentato dall'**informativa** (art. 13) che ciascun interessato deve ricevere prima della raccolta o della registrazione dei dati non raccolti presso l'interessato, ossia provenienti da altre fonti.

L'informativa deve riguardare:

- le finalità e le modalità del trattamento cui sono destinati i dati
- la natura obbligatoria o facoltativa del conferimento dei dati
- le 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 in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi
- i diritti di cui all'art. 7
- gli estremi identificativi del titolare e del responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art. 7, se designato.

La suddetta informativa più essere fornita all'interessato anche solo verbalmente, tenuto conto, in tale caso, delle difficoltà di prova, a posteriori, di aver adempiuto all'obbligo.

Il trattamento di dati personali è inoltre legittimo solo con il **consenso espresso dell'interessato** (art. 23) e il consenso si considera validamente prestato solo se preceduto dall'informativa di cui sopra e se è documentato dall'impresa per iscritto.

Il consenso deve invece essere **manifestato in forma scritta** dall'interessato quando il trattamento riguarda **dati sensibili** (art. 4, c. 1, lett. d). A tale proposito si ricorda che per dati sensibili si intendono alcuni dati personali **specificamente individuati dalla legge**, tra cui sono compresi i dati personali idonei a rivelare lo **stato di salute**.

La legge prevede espressamente alcuni casi che fanno eccezione alla regola generale, in cui possono essere effettuati trattamenti di dati personali **senza il consenso** dell'interessato (art. 24).

All'**interessato** sono riconosciuti i seguenti **diritti** (art. 7), ai quali il titolare deve fornire **riscontro senza ritardo**:

- ottenere la conferma dei dati personali trattati dal titolare e la loro comunicazione in forma intelligibile
- ottenere l'indicazione :
    - dell'origine dei dati personali
    - delle finalità e delle modalità del trattamento
    - della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici
    - degli estremi identificativi del titolare e dei responsabili
    - dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati
- ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati
- ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati
- ottenere l'attestazione che le operazioni di cui sopra sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha diritto di opporsi, in tutto o in parte:

- per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Oltre a quanto sin qui illustrato, chi effettua trattamenti di dati personali è tenuto ad applicare le **misure di sicurezza dei dati e dei sistemi**.

La legge stabilisce (art. 31) che i dati personali trattati debbano essere custoditi e controllati in modo da **ridurre al minimo i rischi** di: distruzione o perdita, anche accidentale, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta. A tal fine l'impresa è tenuta ad adottare **misure di sicurezza preventive e idonee**, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento. Le misure di sicurezza che devono essere poste a protezione dei dati personali sono rappresentate da **strumenti e accorgimenti tecnici e organizzativi** determinati sulla base dell'analisi dei rischi.

Prerequisito essenziale per procedere legittimamente al trattamento dei dati personali è l'adozione delle **misure minime di sicurezza** di cui all'allegato B del Codice della privacy, volte ad assicurare un livello minimo di protezione dei dati personali, sia in relazione al **trattamento di dati personali mediante strumenti elettronici** sia al trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici (art. 34).

Considerato che gran parte degli adempimenti in tema di misure di sicurezza spettano all'**amministratore di sistema** (figura prevista dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, in bollettino n. 99 novembre 2008), l'impresa può affidare tale compito a un soggetto esterno che, per competenza, esperienza e affidabilità, fornisce idonea garanzia del pieno rispetto della legge, ivi compreso il profilo della sicurezza (viene appunto nominato amministratore di sistema e conseguentemente contrattualizzato). L'operato degli amministratori di sistema deve essere verificato dal titolare con cadenza almeno annuale.

La **violazione delle norme in tema di tutela della privacy** comporta l'applicazione di sanzioni di carattere penale, civile e amministrativo. Quanto alla responsabilità penale, si consideri che il **trattamento di dati personali senza il consenso dell'interessato** può essere sanzionato, in particolari circostanze, con la reclusione fino a 24 mesi (art. 167, c. 1). Quanto alla responsabilità amministrativa, l'**omessa o inidonea informativa all'interessato** comporta l'applicazione di una sanzione pecuniaria sino a € 36.000 (sanzione aumentabile sino al quadruplo ai sensi dell'art. 164 *bis*). In termini civilistici infine, per i danni cagionati per effetto del trattamento di dati personali, è posta a carico dell'impresa (art. 15) la responsabilità aggravata prevista per l'esercizio di attività pericolose (art. 2050 codice civile): il responsabile è liberato solo se **prova di avere adottato tutte le misure idonee a evitare il danno**. Nel caso in cui l'illecito consista nella violazione dei principi di corretto trattamento (art. 11), è prevista anche la risarcibilità del **danno non patrimoniale**.

Come anticipato sopra, dal **25 maggio 2018**, sarà applicabile alla materia il **Regolamento UE 2016/679** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (www.garanteprivacy.it). Tale Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali.

Il Regolamento conferma che il trattamento di dati personali è **lecito** solo se, e nella misura in cui, ricorrono le condizioni di cui al suo articolo 6, che coincidono sostanzialmente con quelle attualmente previste dal Codice, in particolare che l'interessato abbia espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità o che il trattamento sia necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dell'interessato stesso oppure che il trattamento sia necessario per adempiere ad un obbligo di legge al quale è soggetto il titolare del trattamento (ossia, nel nostro caso, l'impresa che effettua l'attività di e-commerce).

Il **consenso** al trattamento dei dati personali deve, quindi, come già secondo il Codice della privacy, essere una manifestazione di volontà dell'interessato libera, specifica, informata e inequivocabile, con la quale l'interessato manifesta, mediante dichiarazione o azione positiva inequivocabile, il proprio

assenso a che i dati personali che lo riguardano siano oggetto di trattamento (articolo 4.11 del Regolamento), non è quindi ammesso il consenso tacito o presunto (ad esempio moduli con caselle pre-spuntate). Per quanto attiene ai **dati personali** che il Codice della privacy definiva **"sensibili"**, con terminologia non ripresa dal Regolamento (articolo 9.1), ossia i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, a differenza di quanto previsto dal Codice della privacy, il consenso non deve necessariamente essere espresso in forma scritta né documentato per iscritto, seppure sia onere del titolare provare che l'interessato abbia prestato il consenso ad uno specifico trattamento (articolo 7.1 del Regolamento). Inoltre la richiesta di consenso all'interessato deve essere formulata in modo comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro e, se ciò avviene nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso al trattamento di dei dati personali deve essere presentata in modo chiaramente distinguibile dalle altre materie. La dichiarazione in violazione del Regolamento non è vincolante (articolo 7.2 del Regolamento). Secondo il Regolamento (articolo 8), inoltre, il consenso al trattamento dei dati personali può essere validamente prestato dai **minori** a partire dai sedici anni, fatte comunque salve le norme vigenti negli Stati membri sull'età per la valida stipulazione dei contratti.

L'**informativa**, come già secondo il Codice della privacy, deve essere fornita all'interessato prima della, o contestualmente alla, raccolta dei dati (articolo 13 del Regolamento, che riguarda i dati raccolti presso l'interessato) e, se i dati non sono raccolti presso l'interessato (articolo 14 del Regolamento), l'informativa deve indicare anche le categorie di dati personali oggetto di trattamento. Nel caso di dati personali non raccolti presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole, non superiore ad un mese, dall'ottenimento dei dati personali oppure, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato o con un terzo, al più tardi al momento della prima comunicazione a questi ultimi. Come in precedenza, nell'informativa il titolare deve indicare l'identità e i dati di contatto propri e, ove applicabile, del suo rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati, se esiste un responsabile del trattamento, la sua identità, e quali sono i destinatari dei dati. Il Regolamento prevede inoltre che il titolare debba indicare l'identità e i dati di contatto del **responsabile della protezione dei dati**, ove applicabile, la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, attraverso quali strumenti. Il Regolamento prevede anche ulteriori informazioni in quanto necessarie per garantire un trattamento corretto e trasparente: in particolare, il titolare deve specificare il **periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo. Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato. Il Regolamento specifica in maggiore dettaglio rispetto al Codice della privacy le **modalità** dell'informativa, che deve avere una forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice e, per i minori, occorre prevedere informative idonee. L'informativa deve essere data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi on line, articolo 12.1), anche se sono ammessi altri mezzi, quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (articolo 12.1). Il Regolamento ammette, ma solo in combinazione con

l'informativa estesa (articolo 12.7), l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, icone che dovranno essere identiche in tutta l'UE e dovranno essere definite dalla Commissione europea.

É necessario che le imprese verifichino la rispondenza alle nuove prescrizioni del Regolamento dei testi di **informativa** utilizzati e dei **consensi** raccolti prima del 25 maggio 2018: i consensi raccolti precedentemente al 25 maggio 2018 resteranno validi solo se pienamente conformi al Regolamento, diversamente le imprese dovranno provvedere, prima di tale data, a raccogliere dagli interessati un nuovo consenso, previa modifica o integrazione dell'informativa. E' anche opportuno che le imprese si organizzino per favorire l'**esercizio dei diritti degli interessati** e per fornire loro riscontro, il che dovrà avvenire, in linea generale, in forma scritta (anche elettronica).

I **diritti dell'interessato** sono oggetto degli articoli da 15 a 22 del Regolamento. Quanto al **diritto d'accesso** (articolo 15), ossia il diritto dell'interessato di ottenere dal titolare la conferma del trattamento di suoi dati personali eventualmente in corso, di avere accesso ai suoi dati personali trattati e di ricevere diverse informazioni relative al trattamento, si segnala l'obbligo del titolare di indicare, quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non possibile, i criteri utilizzati per determinare tale periodo nonché l'obbligo del titolare di fornire all'interessato una copia dei dati personali trattati ed il suo diritto di addebitare un contributo spese ragionevole basato sui costi amministrativi in caso di richiesta di ulteriori copie. Inoltre, ove possibile, i titolari dovrebbero fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali (Regolamento, considerando 23). L'interessato ha inoltre, come già secondo il Codice della privacy, il **diritto di rettifica** e integrazione dei dati personali inesatti, cui il titolare deve provvedere su richiesta dell'interessato senza ingiustificato ritardo (articolo 16 del Regolamento). Il diritto di cancellazione (cosiddetto "**diritto all'oblio**", di cui all'articolo17 del Regolamento) risulta rafforzato rispetto al Codice della privacy, innanzitutto con la previsione dell'obbligo dei titolari che abbiano reso pubblici i dati (ad es. tramite pubblicazione web) di cancellarli e di informare della richiesta dell'interessato i titolari del trattamento che stanno trattando tali dati personali al fine della cancellazione qualsiasi link, copia o riproduzione dei dati. Inoltre l'interessato ha il diritto di richiedere la cancellazione dei propri dati personali anche dopo revoca del consenso al trattamento, se non sussiste altro fondamento giuridico per il trattamento. È inoltre previsto il **diritto alla limitazione del trattamento** (articolo 18 del Regolamento), diritto diverso e più esteso rispetto al "blocco" del trattamento previsto dal Codice della privacy, esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati) ma anche nel caso in cui l'interessato richieda la rettifica dei dati o si opponga al loro trattamento fintantoché il titolare non provveda. In caso di limitazione, i dati possono essere trattati unicamente con il consenso dell'interessato, salva la conservazione, la difesa in giudizio, la difesa dei diritti di un terzo o per motivi di interesse pubblico. È poi previsto un **obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento** (articolo 19 del Regolamento), in base al quale il titolare deve comunicare i predetti interventi a tutti i destinatari cui sono stati trasmessi i dati personali (salvo che ciò sia impossibile o implichi uno sforzo sproporzionato), dovendo altresì comunicare, all'interessato che lo richieda, chi sono tali destinatari. È infine previsto un nuovo **diritto alla portabilità dei dati** (articolo 20 del Regolamento) che consiste nel diritto dell'interessato di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico (il diritto non si applica, infatti, ai dati cartacei), i dati personali che lo stesso ha fornito

ad un determinato titolare e di trasmetterli, senza impedimenti da parte di quest'ultimo, a un altro titolare del trattamento. L'interessato ha anche il diritto di ottenere la trasmissione diretta dei dati personali da un titolare all'altro, se tecnicamente fattibile. Si noti che sono oggetto di questo diritto solo i dati trattati con mezzi automatizzati e con il consenso dell'interessato o in base ad un contratto con l'interessato, e solo i dati che siano stati forniti al titolare dall'interessato. L'interessato ha poi il **diritto di opposizione** al trattamento dei suoi dati personali alle condizioni di cui all'articolo 21 del Regolamento nonché il **diritti relativi ai processi decisionali automatizzati, compresa la profilazione** (articolo 22 del Regolamento). L'interessato ha infatti 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, salvo che la decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento oppure si basi sul consenso esplicito dell'interessato oppure sia autorizzata dalla legge. Nei primi due casi, il titolare attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Come già per l'informativa sul trattamento dei dati personali, anche per quanto riguarda i **diritti dell'interessato**, il titolare del trattamento deve, in base all'articolo 12 del Regolamento, adottare misure appropriate per informare quest'ultimo dei suoi diritti sopra esposti (articoli da 15 a 22 del Regolamento). Detta informativa, così come il riscontro all'interessato in caso di esercizio dei diritti, deve avvenire in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Il riscontro all'interessato deve, di regola, avvenire in forma scritta, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, può essere dato oralmente solo se così richiede l'interessato stesso (artt. 12.1 e 15.3 del Regolamento). Il titolare del trattamento è tenuto ad agevolare l'esercizio dei diritti dell'interessato. Il titolare del trattamento è tenuto a fornire riscontro all'interessato che eserciti i suoi diritti senza ingiustificato ritardo e, comunque, al più tardi entro un mese (prorogabile a due in casi di particolare complessità e di richieste numerose). L'esercizio dei diritti deve di norma essere gratuito per l'interessato ma in caso di richieste manifestamente infondate o eccessive o ripetitive (carattere che è onere del titolare provare) oppure se sono richieste più copie dei dati personali, in caso del diritto di accesso (articolo 15.3 del Regolamento), il titolare del trattamento può addebitare un contributo spese ragionevole oppure rifiutare di soddisfare la richiesta.

Quanto ai soggetti della normativa in questione, il Regolamento definisce caratteristiche soggettive e responsabilità di **titolare** e **responsabile** del trattamento negli stessi termini di cui al Codice della privacy. Non viene invece più definita la figura dell'incaricato del trattamento ma si contempla ovviamente l'esistenza di persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (articolo 4.10 del Regolamento). Il Regolamento invece disciplina la situazione **contitolarità** (articolo 26), che si verifica quanto due o più titolari del trattamento si trovano a determinare congiuntamente le finalità e i mezzi del trattamento. Essi devono determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità anche in merito ai rapporti con gli interessati (con particolare riguardo all'esercizio dei diritti e alle informative di cui agli articoli 13 e 14), ai quali deve essere messo a disposizione il contenuto essenziale di tale accordo, che può designare un punto di contatto per gli interessati, sebbene l'interessato possa comunque esercitare i propri diritti nei confronti di ciascun titolare. Il titolare può nominare

unicamente **responsabili** del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate (l'adesione a codici deontologici può valere a provare le "garanzie sufficienti"). Anche per quanto riguarda i rapporti con i responsabili del trattamento, il Regolamento (articolo 28.3) richiede che siano disciplinati da un contratto che stabilisca la natura, la durata e la finalità dei trattamenti assegnati, il tipo di dati personali e le categorie di interessati, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni necessariamente impartite dal titolare (articolo 29 del Regolamento) e, in generale, delle disposizioni del Regolamento. Il Regolamento pone in capo ai responsabili del trattamento degli obblighi specifici, distinti da quelli previsti in capo ai titolari, quali la tenuta del registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare (articolo 30.2), l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (articolo 32), la designazione di un responsabile della protezione dei dati nei casi previsti (articolo 37). Si prevede anche che il responsabile possa nominare, rispondendone nei confronti del titolare, un sub-responsabile per l'esecuzione di specifiche attività di trattamento: ciò deve avvenire alle medesime condizioni alle quali il responsabile è stato nominato dal titolare. Si ricorda che il responsabile del trattamento (così come il titolare del trattamento) è esonerato dalla responsabilità per i danni cagionati da trattamenti illegittimi unicamente se dimostra che l'evento dannoso non gli è in alcun modo imputabile (articolo 82 del Regolamento).

Si consiglia alle imprese titolari di trattamento di valutare l'esistenza di eventuali situazioni di **contitolarità** e, in tali casi, stipulare l'accordo interno previsto dal Regolamento, nonché verificare che i contratti con i loro responsabili siano conformi a quanto previsto dal Regolamento, apportando le integrazioni o modifiche necessarie entro il 25 maggio 2018.

Il Regolamento punta in particolare alla **responsabilizzazione** ("accountability") **dei titolari**, i quali sono tenuti a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alle norme e ai criteri stabiliti dal Regolamento (articolo 24). Fondamentale criterio è quello della **protezione dei dati fin dalla progettazione e dalla protezione per impostazione predefinita** ("data protection by default and by design" di cui all'articolo 25), ossia la necessità che il titolare configuri il trattamento, sin dal momento della determinazione dei suoi mezzi e all'atto del trattamento stesso, mettendo 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 garanzie necessarie al fine di soddisfare i requisiti del Regolamento.

Quanto alle principali novità in termini di **adempimenti** da parte di titolari e responsabili del trattamento, ricordiamo il **registro dei trattamenti**, non obbligatorio per le imprese con meno di 250 dipendenti (salvo che effettuino trattamenti rischiosi), ma comunque consigliabile per tutti, ove annotare le operazioni di trattamento secondo i contenuti minimi di cui all'articolo 30. Quanto alle **misure di sicurezza** il Regolamento stabilisce (articolo 32) che il titolare e il responsabile debbano mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, fornendone un elenco esemplificativo. Anche in questo caso, l'adesione a codici di condotta (articolo 40) può valere per dimostrare la conformità delle misure di sicurezza al Regolamento. Quanto alla **notifica delle violazioni di dati personali** all'autorità di controllo sarà obbligatoria, a partire dal 25 maggio 2018, per tutti i titolari, che dovranno procedervi, con i

contenuti minimi previsti dal Regolamento (articolo 33), senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sono venuti a conoscenza, a meno che sia improbabile (valutazione rimessa al titolare) che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Quando poi tale rischio sia elevato, la violazione deve essere comunicata, senza ingiustificato ritardo, anche all'interessato (articolo 34), descrivendo con linguaggio semplice e chiaro la natura della violazione dei dati personali e contenente almeno le informazioni e le misure di cui all'articolo 33. La comunicazione all'interessato non è richiesta se il titolare aveva applicato ai dati personali oggetto della violazione misure tecniche e organizzative di protezione adeguate (es. la cifratura dei dati) o se 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 o se la comunicazione richiederebbe sforzi sproporzionati, dovendosi in tal caso procedere invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati siano informati con analoga efficacia.
Sulla comunicazione della violazione e su tutta la disciplina in materia, il Comitato europeo della protezione dati è chiamato a formulare linee-guida specifiche ed inoltre l'Autorità garante per la protezione dei dati personali ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico che si intende rielaborare al fine di renderlo utilizzabile da tutti i titolari di trattamento.

Tutti i titolari di trattamento devono in ogni caso documentare qualsiasi **violazione di dati** personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati per porvi rimedio (articolo 33.5), è quindi necessario che i titolari di trattamento adottino le misure necessarie a documentare eventuali violazioni, essendo tenuti a fornire tale documentazione al Garante, in caso di accertamenti.

In aderenza all'approccio di responsabilizzazione dei titolari cui è improntato il Regolamento, esso prevede (articolo 37) la nomina di un **responsabile della protezione dati** ("**Data Protection Officer**"), che è obbligatoria, oltre che per i soggetti pubblici, per i titolari le cui principali attività consistano in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure consistono nel trattamento, su larga scala, di categorie particolari di dati personali (dati "sensibili" di cui all'articolo 9.1 e i dati "giudiziari" 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 privacy, e della capacità di assolvere i compiti previsti dal Regolamento, può essere un dipendente del titolare o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. Il Regolamento detta poi una serie di norme volte a tutelare l'efficacia dell'attività del responsabile della protezione dei dati, quali l'obbligo di coinvolgerlo in tutte le questioni riguardanti la privacy, di sostenerlo con le risorse necessarie, di assicurargli l'indipendenza, non potendo essere rimosso o penalizzato per l'adempimento dei propri compiti e riferendo direttamente al vertice gerarchico del titolare. Il responsabile della protezione dei dati è tenuto al segreto, può svolgere al contempo altri compiti e funzioni, che tuttavia il titolare assicura che non diano adito ad un conflitto di interessi (articolo 38). Il responsabile della protezione dei dati è incaricato di informare e fornire consulenza al titolare o al responsabile del trattamento nonché ai relativi dipendenti che eseguono le operazioni

di trattamento, sorvegliarne l'osservanza degli obblighi di legge nonché di cooperare con l'autorità di controllo (articolo 39).

Per quanto riguarda il **trasferimento dei dati personali all'estero**, il Regolamento stabilisce che il trasferimento può avvenire senza l'autorizzazione nazionale dell'Autorità Garante se verso un Paese terzo che, secondo la Commissione europea, garantisca un livello di protezione adeguato (articolo 45) oppure se il titolare abbia fornito garanzie adeguate, tra cui clausole tipo di protezione dei dati adottate dalla Commissione europea o dall'Autorità Garante oppure codici di condotta o meccanismi di certificazione (unitamente ad un impegno vincolante del titolare mediante uno specifico strumento contrattuale o un altro strumento che sia giuridicamente azionabile dagli interessati) o ancora clausole contrattuali tra il titolare o il responsabile e il destinatario dei dati nel paese terzo (articolo 46) oppure se l'interessato, informato della situazione e dei rischi, abbia esplicitamente acconsentito al trasferimento o se il trasferimento sia necessario all'esecuzione di un contratto tra il titolare e l'interessato (o comunque in suo favore) oppure all'esecuzione di misure precontrattuali adottate su richiesta dell'interessato (articolo 49) o in altri casi qui non rilevanti.
Per quanto riguarda i flussi di dati personali al di **fuori dell'Unione Europea e dello Spazio Economico Europeo**, il Regolamento ha poi confermato l'approccio del Codice della privacy, risalente alla Direttiva 95/46/CE e al Codice italiano, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie previste dal Regolamento.