Diritto alla protezione dei dati personali

La tutela dei dati personali è diventata, oggi, un settore chiave per le aziende del web. Il dato personale è il metro di misura di un servizio o di un prodotto, da cui l'esigenza di una regolamentazione a tutela dei diritti dei cittadini e in particolare del **diritto alla protezione dei dati** (*data protection*).
Questo diritto si è sviluppato a partire dal **diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza**. La dignità della persona umana, infatti, è il valore dominante di tutte le carte dei diritti.
E' previsto dall'articolo 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU) e dall'articolo 16 del TFUE (Trattato sul funzionamento dell'Unione europea), e costituisce un **diritto fondamentale dell'individuo**, appartiene alle sole persone fisiche e in genere alle persone viventi, ed è un diritto autonomo rispetto al più generale diritto alla riservatezza (privacy).
Il **diritto alla riservatezza** ha un'accezione prevalentemente negativa (*ius excludendi alios* dalla propria vita privata), in quanto è volto a non far rilevare informazioni sul nostro conto, essendo legato alla stessa concezione che è alla base del diritto di proprietà. Non è quindi pensato come un diritto a sé ma nasce come **limite alla libertà di espressione e al diritto all'informazione**, quindi è il diritto a che non vengano diffuse informazioni personali, a mezzo stampa o tramite i media, senza che la persona interessata abbia dato il suo consenso, a meno che la notizia ad essa riferita sia di pubblico interesse.

Diritto fondamentale
Mentre la privacy rappresenta una sorta di diritto individuale, che tutela il singolo nella sua solitudine, il **diritto alla protezione dei dati personali**, invece, estende la tutela dell'individuo oltre la sfera della vita privata e in particolare nelle relazioni sociali, così garantendo l'**autodeterminazione decisionale e il controllo sulla circolazione dei propri dati**. Si tratta, quindi, di garantire la libertà personale come diritto fondamentale, non solo come libertà fisica ma anche contro ogni controllo illegittimo e ogni ingerenza altrui, e trova la sua maggiore espressione nell'Europa che ha conosciuto le dittature del Novecento, e quindi come contrapposizione contro non solo i giornali e i media ma, anche e soprattutto, gli Stati autoritari.
In base alla normativa che regolamenta tale diritto, quindi, ogni individuo può pretendere che i suoi dati personali siano raccolti e trattati da terzi solo nel rispetto delle regole e dei principi previsti dalle leggi in materia, sia dell'Unione Europea che dei singoli Stati nazionali. Lo scopo della normativa è quello di attribuire al solo interessato il potere di disporre dei propri dati, assicurando all'individuo il controllo su tutte le informazioni riguardanti la sua vita privata, e fornendogli nel contempo gli strumenti per la tutela di queste informazioni.
Il diritto alla protezione dei dati personali è sancito da numerose norme internazionali, dell'Unione Europea e dei singoli Stati membri dell'Unione. Ad esempio l'articolo 12 della Dichiarazione universale dei diritti dell'uomo (UDHR) delle Nazioni Unite (ONU), che per la prima volta nel 1948 ha previsto tale diritto influenzando la nascita dei successivi strumenti legislativi. Inoltre è sancito nella Carta dei diritti dell'Unione europea (Carta di Nizza) proclamata nel 2000.
Oggi è un **diritto fondamentale autonomo**, come proclama esplicitamente il nuovo regolamento europeo in materia, che deve coesistere con gli altri diritti, compresa la libertà di stampa e di manifestazione del pensiero.

Principi
La protezione dei dati personali si basa su 8 principi che reggono l'elaborazione dei dati:

1. Raccogliere e elaborare i dati in modo equo;
2. Conservare i dati solo per le finalità specificate, esplicite e legittime;
3. Utilizzare e divulgare i dati solo in modi compatibili con le finalità prefissate;
4. Tenere i dati al sicuro;
5. Mantenere i dati aggiornati e completi;
6. Assicurarsi che i dati siano adeguati, pertinenti e non eccessivi;
7. Conservare i dati solo per il tempo necessario per le finalità prefissate;
8. Fornire una copia dei suoi dati personali a richiesta degli interessati.

L'interessato

L'interessato (*data subject*) al trattamento è la persona fisica a cui si riferiscono i dati personali.
L'interessato è una **persona fisica identificata o identificabile**, cioè che può essere identificata anche in modo indiretto, facendo riferimento a informazioni o elementi caratteristici, o tramite l'incrocio di più dati personali.
L'interessato deve essere necessariamente una persona fisica. Per quanto riguarda l'Italia, il Decreto Legge 6/12/2011 n. 201 (decreto Salva Italia del governo Monti) ha chiarito che le imprese e gli enti non possono più essere considerati interessati al trattamento, per cui non potranno esercitare i relativi diritti.

Diritti dell'interessato
La normativa attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi direttamente al titolare del trattamento. L'interessato può esercitare i suoi diritti anche in un momento successivo a quello in cui ha prestato il consenso, potendo così revocare un consenso già prestato.

I diritti esercitabili dall'interessato sono i seguenti:

- esercitare l'**opposizione** al trattamento in tutto o in parte;
- ottenere la **cancellazione** dei dati in possesso del titolare;
- ottenere l'aggiornamento o la rettifica dei dati conferiti;
- chiedere ed ottenere in forma intellegibile i dati in possesso del titolare (diritto di **accesso**);
- chiedere ed ottenere **trasformazione in forma anonima** dei dati;
- chiedere ed ottenere il **blocco o la limitazione** dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento.

Diritto di opposizione
L'interessato ha il diritto di opporsi, in qualsiasi momento al trattamento dei dati che lo riguardano (Art. 21 GDPR).
L'interessato può opporsi anche ai trattamenti connessi a ragioni di interesse pubblico o posti in essere per il perseguimento di interessi legittimi del titolare del trattamento o di terzi. Si tratta di un diritto che trova la sua ragione di essere nella tutela dell'individuo dal controllo eccessivo dello Stato.
L'interessato può opporsi anche al **trattamento dei dati per fini commerciali**, come marketing diretto e profilazione.

L'opposizione al trattamento è operazione diversa dalla cancellazione dei dati. In base ad essa l'interessato può impedire il trattamento che non è compatibile con le finalità del consenso.
E' il titolare del trattamento che deve dare riscontro alla richiesta dell'interessato, entro un mese dall'esercizio del diritto. In casi particolarmente complessi la risposta può essere fornita entro 3 mesi. La risposta deve aversi in forma scritta, anche in formato elettronico, tranne nel caso in cui l'interessato la richieda oralmente. La risposta deve essere coincisa, accessibile ed intellegibile. L'unico obbligo per l'interessato è di fornire i dati per la sua identificazione. La risposta in genere dovrebbe essere senza costi, tranne l'eventuale rimborso del costo del supporto utilizzato.

Diritto di informazione
L'interessato al trattamento ha innanzitutto il diritto a ricevere una corretta informazione in relazione ai dati raccolti e trattati, alle finalità del trattamento, alla base giuridica del trattamento e ai diritti che gli sono attribuiti, nonché le modalità per esercitarli. Tutto ciò avviene a mezzo dell'informativa, il cui scopo è informare l'interessato che così possa rendere un valido consenso.
Nel caso in cui ai dati sia applicato un trattamento automatizzato comprendente profilazione il titolare deve informare l'interessato, esplicitando le modalità e le finalità della profilazione, nonché la la logica inerente il trattamento e le conseguenze previste per l'interessato a seguito di tale tipo di trattamento.

Diritto di accesso
L'art. 15 del regolamento generale europeo prevede il diritto di accesso, cioè il diritto di conoscere quali dati personali relativi all'interessato il titolare sta trattando, con quali finalità (non le modalità invece), e di ricevere una copia (gratuita) dei dati. I titolari possono eventualmente anche consentire un accesso diretto ai dati da remoto.

L'interessato ha il diritto di conoscere:

- le finalità del trattamento;
- le categorie di dati personali trattate;

- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali, e le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi;
- quando possibile, il **periodo di conservazione dei dati** personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- l'esistenza del diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un **processo decisionale automatizzato**, compresa la profilazione, e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate rispetto alla tutela fornita nel paese terzo.

Diritto di limitazione del trattamento
Il diritto di limitazione (art. 18 del Regolamento) consente all'interessato di ottenere il blocco del trattamento in caso di violazione dei presupposti di liceità (quale alternativà alla cancellazione dei dati stessi), ma anche se l'interessato chiede la rettifica dei dati (in attesa della rettifica) o si oppone al loro trattamento (in attesa della decisione del titolare). In caso di esercizio di tale diritto ogni trattamento, tranne la conservazione, è vietato.
Il dato deve essere **contrassegnato** in attesa delle ulteriori valutazioni.

Diritto alla cancellazione (oblio)
Il diritto di cancellazione (anche detto diritto "all'oblio") è il diritto di ottenere la cancellazione dei propri dati personali in casi particolari. Può essere esercitato anche dopo la revoca del consenso.

Diritto alla portabilità
Il diritto alla portabilità dei dati è un nuovo diritto previsto dal regolamento europeo. Si applica solo ai trattamenti automatizzati, e sono previste specifiche condizioni per il suo esercizio.

Esercizio dei diritti
L'interessato può rivolgersi direttamente al titolare del trattamento per l'esercizio dei suoi diritti (interpello). Anche se è solo il titolare obbligato a dare riscontro, il responsabile del trattamento è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti.
In caso di mancata risposta, o di risposta inadeguata, può rivolgersi all'autorità amministrativa (Garante) o giudiziaria per la tutela dei suoi diritti.
Il termine per la risposta è di **1 mese** per tutti i diritti. Tale termine può essere esteso a **3 mesi** in casi di partiolare complessità. In questo caso il titolare del trattamento deve comunque avvertire l'interessato entro il mese.
L'esercizio dei diritti è in linea di massima **gratuito**. Spetta comunque al titolare valutare se la risposta è complessa al punto da dover chiedere un **contributo** all'interessato, e stabilirne l'ammontare, ma solo se si tratta di richieste manifestamente infondate o eccessive o ripetitive (sul punto il Garante italiano dovrebbe pubblicare delle linee guida, per il momento si può fare riferimento alla delibera del 2004 Contributo spese in caso di esercizio dei diritti dell'interessato).
La risposta si deve fornire di regola in forma scritta, anche attraverso strumenti elettronici. Può essere orale solo se espressamente richeista in tal senso dal'interessato. La risposta deve essere chiara, coincisa, e facilmente accessibile e comprensibile.
Il titolare può chiedere informazioni all'interessato al fine di identificarlo, e l'interessato è obbligato a fornire tali informazioni.

Deroghe ell'esercizio dei diritti
Il regolamento europeo ammette delle deroghe ai diritti riconosciuti all'interessato, da stabilire in base a disposizioni nazionali. In tale prospettiva si ritiene possano essere ancora applicate (in attesa della valutazione del Garante sulla conformità al GDPR) le deroghe stabilire dall'articolo 8 del Codice per la protezione dei dati personali italiano, e cioè nei casi in cui il trattamento dati è effettuato:

a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di **riciclaggio**;
b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di **sostegno alle vittime di richieste estorsive**;

c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) da un **soggetto pubblico**, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per **esclusive finalità inerenti alla politica monetaria e valutaria**, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle **investigazioni difensive o per l'esercizio del diritto in sede giudiziaria**;
f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;
g) per **ragioni di giustizia**, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
h) ai sensi dell'articolo 53 (trattamenti da parte di forze di polizia), fermo restando quanto previsto dalla legge 1 aprile 1981, n. 121.

Titolare del trattamento

Il **Titolare del trattamento** (*data controller*) è colui che "*da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali*" (direttiva 95/46, art. 2 lett. d), e decide quali categorie di dati personali devono essere registrate (Convenzione 08, art. 2 lett. d). O anche, è "*la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza*" (Codice in materia di protezione dei dati personali, art. 4). In sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati.

L'introduzione del nuovo regolamento generale europeo ha creato qualche problema nella traduzione dei termini, in quanto il termine ***data controller*** va tradotto, come stabilito dal Garante italiano, con titolare del trattamento, cioè colui il quale è responsabile per il trattamento medesimo. Questo ha creato qualche confusione col responsabile del trattamento, che invece più correttamente è la traduzione di *data processor*.

Il titolare del trattamento non è, quindi, chi gestisce i dati, ma **chi decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa,** sia nazionale che internazionale, in materia di protezione dei dati personali, compreso l'obbligo di notifica al Garante nei casi previsti.
Tra questi obblighi è importante ricordare che il titolare del trattamento deve porre in essere misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (privacy by design).
E' pacifico che il titolare è sempre vincolato al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento. Quindi egli deve garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente. In tale prospettiva spetta a lui stabilire le misure adeguate di sicurezza.

Il titolare nomina con contratto o atto giuridicamente valido, il responsabile del trattamento, insieme al quale pone in atto le misure tecniche ed organizzative congrue per garantire un livello di sicurezza adeguato al rischio.
Inoltre, il titolare del trattamento, e il responsabile, sono tenuti alla redazione del registro di trattamenti.

Un privato che effettua un trattamento di dati a fini esclusivamente personali non rientra nell'ambito applicativo della direttiva europea in materia di protezione dei dati, e quindi non assume la qualifica di Titolare. Ma la **Corte di Giustizia europea** (CGUE) ha stabilito che comunque **la pubblicazione di dati altrui su Internet costituisce trattamento**, poiché la pubblicazione online determina l'accessibilità da parte di un numero enorme di individui, e quindi si può parlare di diffusione sistematica.

Nel **settore privato** il titolare del trattamento può essere una persona fisica oppure una persona giuridica. Nel **settore pubblico** in genere il titolare del trattamento è l'autorità, cioè una persona giuridica.
Qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il titolare è l'ente nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.) anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.). In molti casi, tali soggetti potrebbero assumere, semmai, la qualifica di "responsabile". Ovviamente non può essere titolare del trattamento un soggetto privo di personalità giuridica propria (Parere del Garante 9 dicembre 1997).
Nel caso di **gruppi di società** la società madre e le controllate sono distinti titolari del trattamento, avendo una personalità giuridica distinta. In tal caso il trasferimento dei dati tra le società del gruppo deve essere autorizzata dagli interessati.

Responsabile del trattamento

Il responsabile del trattamento (data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8).

Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato. Il responsabile del trattamento dovrà avere innanzitutto una competenza qualificata (ad esempio, frequentazione di corsi di aggiornamento), dovendo garantire una conoscenza specialistica della materia, e l'attuazione delle misure tecniche e organizzative in grado di soddisfare i requisiti stabilitl dal regolamento europeo. Inoltre dovrà garantire una particolare affidabilità, un requisito fondato su aspetti etici e deontologici (ad esempio, l'assenza di condanne penali).
Ovviamente dovrà disporre delle risorse tecniche adeguate per l'attuazione degli obblighi derivanti dal contratto di designazione e dalle norme in materia. Se è soggetto interno le risorse saranno a carico del titolare.

Responsabile interno od esterno?
Il ruolo del responsabile del trattamento di cui al regolamento europeo è chiaramente riservato ad un soggetto esterno all'azienda, con riferimento ai fornitori di servizi. Infatti, vi è uno specifico obbligo di predisporre un contratto per la designazione delle responsabilità a carico del responsabile. A livello europeo, inoltre, si è da sempre affermata l'idea che il responsabile del trattamento non possa essere un soggetto alle dipendenze del titolare. Sia l'ICO britannico che il CNIL francese, infatti, richiamano espressamente il parere (1/2010) del Gruppo articolo 29 per evidenziare come il responsabile sia solo un soggetto esterno all'azienda.
In particolare il WP29 ricorda che il titolare del trattamento può decidere di trattare i dati all'interno della propria azienda oppure delegare in tutto o in parte le attività di trattamento dati ad un soggetto esterno. Quindi per agire come responsabile del trattamento occorre essere una persona giuridica distinta dal titolare e elaborare dati per conto di questi.
Quindi, il responsabile del trattamento deve essere esterno all'azienda. Il responsabile del trattamento tratta i dati attenendosi alle istruzioni del titolare, e assume responsabilità proprie e ne risponde alle autorità di controllo e alla magistratura. Il titolare del trattamento, ovviamente, può distribuire incarichi interni (es. responsabile dell'area legale, dell'area marketing, ecc...), ma la responsabilità rimane sua, e dell'eventuale responsabile (esterno) nominato.
Nel caso di gruppi di imprese, un'impresa può agire in qualità di responsabile del trattamento per un'altra impresa.

Situazione in Italia
L'esperienza italiana ha sempre ammesso il responsabile del trattamento interno. In tal senso, con la legge 20 novembre 2017, n. 167 (Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017), il legislatore italiano ha modificato l'articolo 29 del Codice Privacy, mantenendo la possibilità di distinguere tra soggetto interno ed esterno. La nomina del responsabile è, quindi, discrezionale, ma se il titolare si avvale di soggetti esterni deve nominarli responsabili del trattamento.

Contratto di designazione
Il titolare del trattamento può scegliere se avvalersi o meno dell'esternalizzazione del servizio di trattamento dei dati, ma una volta optato per tale soluzione non può fare a meno di nominare il soggetto in questione quale responsabile del trattamento.
In tal senso il titolare del trattamento nomina uno o più responsabili. In base all'art. 28 del nuovo regolamento generale europeo, la nomina deve avvenire tramite contratto o altro "atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e 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".
Il contratto deve, quindi, essere conforme a quanto stabilito dell'art. 28 del nuovo Regolamento Generale. Col contratto il titolare delega al responsabile la concreta gestione del trattamento, affidandogli uno o più compiti specifici oppure una serie di compiti dettagliati in generale. Il responsabile a sua volta può nominare responsabili di secondo livello, a meno che non sia vietato dalle istruzioni del titolare. E' comunque il responsabile principale a rispondere dell'operato degli altri da lui nominati, di fronte al titolare del trattamento.
Il titolare del trattamento rimane, a sua volta, responsabile della gestione effettuata dai responsabili, dovendo garantire che le loro decisioni siano conformi alle leggi, e in particolare il titolare deve scegliere responsabili del trattamento che offrano garanzie sufficiente ed adeguate nell'adozione di idonee misure tecniche e organizzative volte alla protezione dei dati personali. Il titolare deve sempre poter sindacare le decisioni dei responsabili.

Nel caso in cui il responsabile del trattamento ecceda i limiti di utilizzo dei dati fissati dal titolare, il responsabile diventa titolare della gestione illecita dei dati e ne risponde come tale, insieme all'effettivo titolare (in sostanza è come se diventassero contitolari).

Obblighi del responsabile

Innanzitutto il responsabile ha obblighi di trasparenza. In tal senso occorre contrattualizzare il rapporto tra titolare e responsabile, specificando gli obblighi e i limiti del trattamento dati. Il responsabile riceverà, tramite l'atto giuridico (cioè per iscritto), tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi. Inoltre il responsabile del trattamento dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento, e dovrà tenere il registro dei trattamenti svolti (ex art. 30, paragrafo 2, del Regolamento Generale).
Poi, il responsabile ha obblighi di garantire la sicurezza dei dati. Egli deve adottare tutte le misure di sicurezza adeguate al rischio (art. 32 regolamento), tra le quali anche le misure di attuazione dei principi di privacy by design e by default, dovrà garantire la riservatezza, vincolando i dipendenti, dovrà informare il titolare delle violazioni avvenute, e dovrà occuparsi della cancellazione dei dati alla fine del trattamento.
Sia il titolare del trattamento che il responsabile, sono tenuti ad attuare le misure tecniche ed organizzative tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Si tratta di specifici requisiti previsti dal GDPR, che indica alcune misure di sicurezza utili per ridurre i rischi del trattamento, quali la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Inoltre, il responsabile ha l'obbligo di avvisare, assistere e consigliare il titolare. Dovrà, quindi, consentire e contribuire alle attività di revisione, comprese le ispezioni (o audit), realizzate dal titolare del trattamento, dovrà avvisare il titolare se ritiene che un'istruzione ricevuta viola qualche norma in materia, dovrà prestare assistenza al titolare per l'evasione delle richieste degli interessati.
Infine, il GDPR pone anche a carico del responsabile del trattamento l'obbligo di tenuta del registro dei trattamenti.

Sub-responsabile

Il responsabile del trattamento può ricorrere ad un altro responsabile solo se è stato previamente autorizzato (tramite il contratto) dal titolare. Il sub-responsabile dovrà essere nominato tramite contratto o atto giuridico e nel rispetto degli obblighi imposti al primo responsabile del trattamento. E' il primo responsabile che risponde dell'inadempimento dei sub-responsabili, nei confronti del titolare, a meno che non riesca a dimostrare che il danno non è in alcun modo imputabile a lui. Per questo motivo il responsabile deve sempre avvisare il titolare della nomina o modifica di un sub-responsabile.

Responsabilità

Nel caso di trattamento in violazione delle norme del regolamento europeo, il responsabile risponde per il danno cagionato all'interessato, secondo quanto previsto dall'articolo 82 e dal Considerando 28. Il responsabile risponde per il danno causato dal trattamento solo in caso di non corretto adempimento degli obblighi previsti dalle norme in capo al responsabile stesso, oppure se ha agito in modo difforme rispetto alla istruzioni del titolare del trattamento.
Se più titolari o responsabili sono coinvolti nello stesso trattamento e sono responsabili del danno causato, ne rispondono in solido per l'intero danno, al fine di garantire l'intero risarcimento. Ovviamente chi paga l'intera somma avrà diritto di regresso nei confronti degli altri responsabili per la quota.
Il titolare e il responsabile sono esonerati da responsabilità se dimostrano che l'evento dannoso non è imputabile alla loro condotta, o se dimostrano di aver adottato tutte le misure idonee per evitare il danno stesso.

Il web hosting quale responsabile del trattamento

Chiunque gestisce un sito web deve tenere presente che il servizio di web hosting, del quale si serve, è giuridicamente il responsabile del trattamento dei dati (nel contempo, però, è sempre il titolare del trattamento dei propri dati), in quanto il web hosting elabora i dati per conto del titolare. Ciò comporta innanzitutto la necessità di un vero e proprio contratto scritto (o equivalente) tra titolare e web hosting, nel quale sarà precisato cosa può fare il web hosting con i dati e quali misure di sicurezza (tecniche e organizzative) deve predisporre, tenendo conto che devono essere adeguate al rischio valutato. L'hosting dovrà, ovviamente, attenersi alle istruzioni di cui al contratto, anche se rimane una certa discrezionalità, ad esempio nella scelta degli strumenti tecnici ed organizzativi più adatti. E' un punto fondamentale, perché se l'hosting va oltre le istruzioni diventa data controller (cioè titolare) con tutte le conseguenze del caso.

L'hosting deve conservare il registro dei trattamenti effettuati per conto del cliente (titolare), nel quale deve includere il nome e i dati di contatto dei titolari del trattamento dei dati, i suoi responsabili e eventuali incaricati, le categorie dei dati trattati, gli eventuali trasferimenti internazionali di dati, e una descrizione generale delle misure di sicurezza tecniche e organizzative adottate. Dalla tenuta del registro in teoria sarebbero esentate le imprese con meno di 250 dipendenti, ma le esenzioni sono particolarmente stringenti e difficilmente applicabili ad un hosting.
L'hosting, inoltre, ha l'obbligo di notificare al titolare le eventuali violazioni di dati. E' buona prassi, quindi, inserire tale obbligo anche nel contratto (che diventerà violazione legale e contrattuale). Poiché l'obbligo a carico del titolare di notificare la violazione agli interessati scatta a partire dal momento in cui ne viene a conoscenza (tramite la comunicazione da parte dell'hosting, in questo caso), si può utilizzare lo stesso termine del GDPR (72 ore).
Il titolare comunque è responsabile nei confronti delle autorità per eventuali violazioni commesse dal web hosting.
E' pacifico che il web hosting è responsabile del trattamento con riferimento ai soli trattamenti realizzati per conto del gestore del sito (quale titolare), cliente dell'hosting. Ma se l'hosting va oltre i limiti del mandato, trattando i dati al di là delle istruzioni ricevute, ne diventa contitolare.
Nel caso in cui ci si serve di un web hosting che si trova al di fuori dello Spazio Economico Europeo (SEE), siamo in presenza di un vero e proprio flusso transfrontaliero dei dati.

Data Protection Officer

Il **Data Protection Officer** (DPO), o anche **Responsabile per la Protezione dei Dati** (RPD), è una figura introdotta dal nuovo regolamento europeo in materia di protezione di dati personali.
Il DPO in realtà è l'evoluzione del "*privacy officer*", figura prevista dalla direttiva europea 95/46 laddove, all'art. 18, consentiva agli Stati dell'Unione di prevedere semplificazioni o esenzioni nei casi di designazione di un soggetto indipendente che garantisca l'applicazione della normativa. Quindi il DPO è un consulente esperto, che va ad affiancare il titolare nella gestione delle problematiche del trattamento dei dati personali, in tal modo si garantisce che un soggetto qualificato si occupi in maniera esclusiva della materia della protezione dei dati personali, aggiornandosi sui rischi e le misure di sicurezza, in considerazione della crescente importanza e complessità del settore.
Il ruolo di DPO può essere affidato ad **uno dei dipendenti dell'azienda** ma può anche essere **esternalizzato a un fornitore di servizi** (libero professionista o azienda) tramite apposito contratto, nel qual caso dovrà essere nominato anche responsabile del trattamento. È difficilmente immaginabile, infatti, che possa svolgere le sue funzioni senza avere accesso ai dati personali. Può essere una persona fisica o un'organizzazione, e può essere nominato per un gruppo di imprese al fine di ridurre i costi.
L'articolo 38 del GDPR stabilisce che il titolare del trattamento e il responsabile del trattamento si assicurano che il DPO non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. Inoltre, il DPO non può essere rimosso o penalizzato dal titolare o dal responsabile del trattamento per l'adempimento dei propri compiti. Questo proprio a tutela della sua autonomia. In tal senso appare difficile ritenere che tale autonomia sia giustificabile nell'ambito di un rapporto di lavoro dipendente, per cui sarebbe preferibile che il DPO sia un soggetto esterno.
La designazione del DPO riflette il nuovo approccio del regolamento europeo (art. 39), maggiormente responsabilizzante, essendo tale designazione finalizzata a facilitare l'attuazione del regolamento da parte del titolare e del responsabile. **Il ruolo del DPO è di tutelare i dati personali, non gli interessi del titolare del trattamento.** E ciò appare ovvio soprattutto nell'ambito degli enti pubblici e delle aziende che effettuano un monitoraggio su larga scala degli individui. Il DPO deve, infatti, possedere un'adeguata conoscenza delle normative e delle prassi di gestione dei dati personali, e **deve adempiere alle proprie funzioni in piena autonomia ed indipendenza, e in assenza di conflitti di interesse**. In tal senso non può ricoprire tale incarico un soggetto che si trova ai vertici aziendali, quindi in grado di influenzare le scelte adottate in materia di trattamento dei dati.
Ovviamente, titolare e responsabile devono mettere a disposizione del DPO le risorse umane e finanziarie per poter svolgere il suo compito.

Nomina e requisiti
Il DPO è designato (art. 37) dal titolare o dal responsabile del trattamento, in base ad un contratto. La designazione dovrà essere comunicata all'Autorità di controllo nazionale.
Link al Modello di atto di designazione del Data Protection Officer
Link al Modello di atto di comunicazione all'Autorità di controllo della designazione del DPO
Tale designazione è obbligatoria solo in tre casi.
1) Per le **amministrazioni e gli enti pubblici** (eccetto le autorità giudiziarie nell'esercizio delle loro funzioni). Nel regolamento europeo non vi è una definizione di "autorità pubblica", per cui occorrerà interpretare l'indicazione in base al diritto nazionale. In particolare il Gruppo Articolo 29 ha raccomandato la nomina del DPO anche per gli organismi privati incaricati dello svolpimengo di pubbliche funzioni o che comunque esercitano pubblici poteri (es. forniture elettriche, trasporti pubblici).
Per stabilire quali sono gli enti soggetti all'obbligo è preferibile fare riferimento alle legislazioni nazionali.
2) Se l'**attività principale** svolta dal titolare o dal responsabile del trattamento consiste nel trattamento di dati che per la loro natura, oggetto o finalità, richiedono il **controllo regolare e sistematico degli interessati** su larga scala.

Con riferimento all'**attività principale**, il Gruppo di lavoro articolo 29 precisa che occorre tenere presente il legame del "core business" con l'attività di trattamento dati. Per cui, se l'attività principale di un ospedale non è il trattamento dei dati ma la salute dei pazienti, essendo le due attività strettamente collegate, il trattamento dei dati rientrerà nell'alveo delle attività principali, per cui un ospedale dovrà nominare un DPO. Stesso discorso di può fare per una società di vigilanza, dove l'attività di sorveglianza è indissolubilmente legata all'attività di trattamento dei dati personali relativi.
Di contro, anche se nella pratica tutte le imprese trattano dati (es. i pagamenti dei dipendenti), non rientrano nell'obbligo di nomina del DPO se il trattamento dei dati è solo di supporto al "core business".
La nozione di **monitoraggio regolare e sistematico** include non solo tutti i vari strumenti di tracciatura elettronica e profilazione online, ma anche qualsiasi forma di tracciatura in un ambiente offline. Per il WP29, un **monitoraggio è regolare** se avviene di continuo o in un arco temporale ben definito, se ripetuto ad intervalli constanti. Il **monitoraggio**

è sistematico se si verifica in base ad uno schema o quando è organizzato, metodico, prestabilito, o se rientra in un piano generale od una strategia (es. servizi di telecomunicazione, marketing, geolocalizzazione, fidelizzazione, monitoraggio di dati sulla salute e forma fisica attraverso dispositivi indossabili, reindirizzamento di email).

Per stabilire se un **trattamento è su larga scala** il WP29 suggerisce di tenere in considerazione alcuni elementi:
- il numero degli interessati coinvolti (in termini assoluti o in percentuale rispetto alla popolazione di riferimento);
- la quantità dei dati trattati;
- le diverse tipologie di dati trattati;
- la durata del trattamento;
- la portata geografica del trattamento.

In tal senso sono trattamenti su larga scala quello dei dati di viaggio dei soggetti che usano un sistema di trasporto pubblico (es. il monitoraggio tramite carte di viaggio), il trattamento dei dati dei pazienti da parte di un ospedale, il trattamento di dati di geolocalizzazione della clientela per fini statistici, il trattamento dei dati dei clienti di una banca o un'assicurazione, il trattamenti dei dati personali per la pubblicità comportamentale (tramite cookie di profilazione), il trattamento di dati dei fornitori di servizi telefonici o internet. Non sono trattamenti su larga scala quelli del singolo medico o del singolo avvocato.
3) Se l'attività principale consiste nel trattamento su larga scala di dati sensibili, relativi alla salute, alla vita sessuale, genetici, giudiziari e biometrici. Il monitoraggio del comportamento delle persone interessate comprende tutte le forme di monitoraggio e profilazione su Internet, anche ai fini della pubblicità comportamentale.
Il Garante italiano ha precisato che non esiste alcun obbligo di nominare quale DPO dei soggetti che abbiano attestati o con partecipazione a corsi di formazione, né esiste alcun albo professionale, quanto piuttosto necessita l'**approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento**. Secondo l'autorità italiana di controllo è opportuno privilegiare soggetti che dimostrino qualità professionali adeguate alla complessità del compito da svolgere, casomai con esperienze di master o corsi di studio.

Compiti e responsabilità

Il Data Protection Officer ha il compito di informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, sugli obblighi previsti dalle norme in materia e quindi verificarne l'attuazione e l'applicazione. Quindi raccoglie informazioni sui trattamenti svolit, e ne verifica la conformità alle norme.
Se richiesto, potrà fornire pareri ed assistere il titolare in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti.
Inoltre è il punto di contatto, non solo per il Garante ma anche per gli interessati al trattamento, in merito a qualunque problematica connessa ai loro dati o all'esercizio dei loro diritti. Potrà, infine, consultare il Garante anche di propria iniziativa.
Occorre tenere presente che è una prassi consolidata che il DPO abbia il compito di realizzare l'inventario dei trattamenti e tenere il registro degli stessi. Questo nonostante sia il titolare, o il responsabile, ad essere obbligati a tale adempimento e responsabilità nei confronti degli interessati e delle autorità di controllo.
Il DPO non è, però, personalmente responsabile dell'inosservanza degli obblighi in materia di protezione dei dati personali, infatti è compito del titolare (art. 24) mettere in atto le misure tecniche ed organizzative adeguate. **Il DPO risponde solo per lo svolgimento dei suoi obblighi di consulenza ed assistenza nei confronti del titolare**, che è (eventualmente in solido col responsabile) l'unico soggetto responsabile del rispetto della normativa. Il titolare, quindi, potrà solo avanzare pretese risarcitorie basate sulla responsabilità contrattuale, nei confronti del DPO.

Linee guida dell'Autorità di controllo nazionale sul Data Protection Officer (RPD) in ambito pubblico

Incaricato del trattamento

L'**incaricato del trattamento** è la persona fisica autorizzata dal titolare o dal responsabile a compiere operazioni di trattamento dei dati.
Il regolamento europeo non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4).

Nomina e requisiti
L'incaricato è, in sintesi, colui che effettua materialmente le operazioni di trattamento sui dati personali. **Può essere solo una persona fisica,** e **deve agire sotto la diretta autorità del titolare del trattamento**. Questo ci indica che se in teoria è possibile che un incaricato sia un soggetto esterno all'azienda, nella pratica risulterebbe difficile.

E' fondamentale tenere presente che in assenza della nomina di incaricati, qualsiasi operazione svolta dai dipendenti o collaboratori del titolare non sarà qualificata come un utilizzo interno dei dati, bensì come una comunicazione a terzi, con le problematiche del caso (in particolare occorre un consenso specifico). l'Autorità di controllo italiana ha precisato che la mancata designazione degli incaricati è una violazione dell'obbligo di applicazione delle misure minime di sicurezza, da cui deriva una sanzione amministrativa (ai sensi dell'art. 162 comma 2 bis del Codice per la protezione dei dati personali) ed una penale (art. 169 del Codice privacy che punisce chi, essendovi tenuto, omette di adottare le misure minime di sicurezza).
La normativa non prevede requisiti quantitativi, per cui anche la semplice presa visione di un dato personale (es. il magazziniere che consulta la bolla di consegna, il portantino che trasporta il malato e la cartella sanitaria) si qualifica come trattamento, e quindi necessita di un formale incarico perché non sia considerato illecito. Ugualmente, non rileva la circostanza che l'incarico sia a pagamento o gratuito, e nemmeno se il collaboratore è esterno (es. il lavoratore chiamato a riparare il computer che, ovviamente, può accedere ai dati ivi contenuti) invece che inquadrato nell'azienda.
La nomina dell'incaricato o degli incaricati (può avvenire anche con unico atto per più incaricati) deve avvenire con **forma scritta, tramite atto nel quale sono indicati i nominativi e i compiti**, compreso gli obblighi inerenti le misure di sicurezza. L'incaricato deve, ovviamente, attenersi streattamente alle istruzioni ricevute. La designazione non necessita di firma degli incaricati per accettazione, anche se è utile una presa visione quale prova della conoscenza dell'incarico.
In alcuni casi può sorgere il dubbio se **designare un incaricato oppure nominare un responsabile**. In genere ci si può orientare verso la nomina di responsabile quando, con riferimento alla quantità di dati e alla criticità degli stessi, appare necessaria una maggiore responsabilizzazione del soggetto, anche in ragione della maggiore autonomia operativa che può essergli concessa in via di una sua particolare specializzazione. L'incaricato, invece, è un mero esecutore di compiti.

Per fare qualche esempio, colui il quale elabora le paghe generalmente va designato responsabile, mentre chi si occupa della manutenzione e dell'assistenza del sistema informatico sarà incaricato. Se però si tratta di una azienda alla quale è affidata la manutenzione dei computer, che quindi manda all'occorrenza diversi soggetti, è preferibile nominare l'azienda stessa quale responsabile esterno, in modo che non occorra nominare caso per caso incaricati le persone inviate per le operazioni.

Trattamento dei dati personali

L'articolo 4 del nuovo Regolamento generale definisce il **trattamento dei dati personali** come qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Tipi di trattamento
La **raccolta** dei dati è la prima operazione e generalmente rappresenta l'inizio del trattamento. Consiste nell'attività di acquisizione del dato.
La **registrazione** consiste nella memorizzazione dei dati su un qualsiasi supporto.
L'**organizzazion**e consiste nella classificazione dei dati secondo un metodo prescelto.
La **strutturazione** consiste nell'attività di distribuzione dei dati secondi schemi precisi.
La **conservazione** consiste nel mantenere memorizzate le informazioni su un qualsiasi supporto.
La **consultazione** è la mera lettura dei dati personali. Anche la mera visualizzazione dei dati è un trattamento che può rientrare nell'operazione di consultazione.
L'**elaborazione** consiste nel'attività con la quale il dato personale subisce una modifica sostanziale. La modificazione differisce dall'elaborazione in quanto può riguardare anche solo parte minima del dato personale.
La **selezione** consiste nell'individuazione di dati personali nell'ambito di gruppi di dati già memorizzati.
L'**estrazione** consiste nell'attività di estrapolazione di dati da gruppi già memorizzati.
Il **raffronto** è un'operazione di confronto tra dati, sia un conseguenza di elaborazione che di selezione o consultazione.
L'**utilizzo** è un'attività generica che ricopre qualsiasi tipo di impiego dei dati.
L'**interconnessione** consiste nell'utilizzo di più banche dati, e si riferisce all'impiego di strumenti elettronici.
Il **blocco** consiste nella conservazione con sospensione temporanea di ogni altra operazione di trattamento.
La **comunicazione** (o cessione) consiste nel dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati. In caso di comunicazione il dato viene trasferito a terzi, ed è quindi attività particolarmente delicata.
Per **diffusione**, invece, si intende il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, diffusione anche quando si pubblica online, ad esempio una fotografia su un social network. In assenza di consenso tale attività deve ritenersi illecita.
La **cancellazione** consiste nell'eliminazione di dati tramite utilizzo di strumenti elettronici.
La **distruzione** è l'attività di eliminazione definitiva dei dati.

Il **trattamento di dati personali** può costituire un'ingerenza con il diritto al rispetto della vita privata, laddove però quest'ultimo diritto non è un diritto assoluto, ma relativo, cioè va contemperato opportunamente con gli altri diritti in gioco, sia privati sia pubblici. Qualsiasi trattamento deve, quindi, essere svolto in maniera lecità e secondo correttezza, i dati devono essere raccolti e trattati per scopi determinati, espliciti e legittimi, e utilizzati in termini compatibili con tali scopi. Inoltre, i dati devono essere esatti e aggiornati, pertinenti, completi e non eccedenti rispetto agli scopi del trattamento. Infine, devono essere conservati per un periodo non superiore al tempo necessario per raggiungere gli scopi del trattamento, trascorso il quale i dati vanno cancellati oppure anonimizzati.
Ovviamente **i dati raccolti o trattati in modo illecito non possono essere in alcun modo utilizzati**. In caso contrario l'utilizzatore può essere soggetto a sanzioni e condannato al risarcimento dei danni causati (art. 2050 cod. civ. e art. 13 Cod. Privacy).

Base giuridica del trattamento
Un trattamento per essere lecito deve trovare fondamento in una idonea base giuridica (consenso,legittimi interessi, ecc...). La normativa prevede, inoltre, che debba essere tenuto un registro dei trattamenti svolti dal titolare, da fornire alle autorità in caso di controllo.

Trattamenti non automatizzati
La regolamentazione della Convenzione 108 e della normativa europea, anche se si concentra principalmente sui trattamenti automatizzati (anche se solo parzialmente), considera anche i trattamenti manuali come oggetto di tutela. In particolare la Convenzione 108 prevede la possibilità che i singoli Stati estendano la definizione di trattamento anche ai trattamenti manuali. I trattamenti non automatizzati sono soggetti alle norme europee se contenuti o destinati a figurare in archivi.

Valutazione di impatto
Una novità prevista dal nuovo regolamento geenerale è data dalla DPIA, la valutazione di impatto del trattamento sui diritti degli interessati, che è diventato un elemento essenziale. Il titolare dovrà valutare il rischio per ogni trattamento, individuando, nei casi di rischio elevato, misure specifiche per l'eliminazione o attenuazione del rischio.

Esenzione per uso personale
Il Codice per la privacy (art. 5) permette, senza necessità di consenso, la raccolta di dati personali per **uso strettamente personale** purché non destinati alla comunicazione o alla diffusione sistematica a terzi (es. pubblicazione sul web). Il caso classico è l'agenda personale, compreso le agende automatizzate. Altre ipotesi di esenzioni si hanno con riferimento agli appunti e al materiale informativo (ritagli da giornali, cd-rom, libri) che chiunque è solito conservare nella propria sfera privata per esigenze culturali o altre esigenze della vita di relazione.
L'eccezione va interpretata, secondo la Corte di Giustizia europea, in senso restrittivo rientrando nella previsione solo un trattamento di dati personali che sia effettuato nella sfera esclusivamente personale o domestica della persona che procede a tale trattamento. Quindi, la pubblicazione di foto online costituisce trattamento soggetto alla normativa in materia di data protection (quindi occorre informativa e consenso).
Il regolamento europeo stabilisce (art. 2 lett c)) che non si applichi ai trattamenti di dati personali "*effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico*". La norma ricalca quella del Codice privacy, senza la delimitazione della destinazione alla comunicazione o diffusione. Questo perché la Corte di Giustizia europea (caso C-101/01 e poi caso C-212/13) ha chiarito che il trattamento di dati personali sul web non può rientrare nell'eccezione delle attività per uso personale e familiare. L'eccezione, in conclusione, deve interpretarsi nel senso che **rientrano in essa solo le attività della vita privata o familiare dei singoli, con esclusione della pubblicazione online che, invece, rende accessibili i dati ad un numero indefinito di persone.**
In realtà il considerando 18 prevede che il regolamento europeo "*non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività*". In tal modo si è ampliata l'eccezione rispetto al passato.
Tuttavia sempre il medesimo considerando stabilisce che il "*presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico*". In tal modo sembra che la responsabilità sia spostata sugli intermediari della comunicazione. In tal senso ricordiamo che l'articolo 2, ultima comma, precisa che "Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva". In questo modo il legislatore chiarisce che il regolamento in materia di protezione dei dati personali non ha effetti giuridici sull'applicazione della direttiva eCommerce (2000/31/CE) e quindi sulle responsabilità in capo ai provider. In tale prospettiva non è chiaro il rapporto tra le due normative.

L'informativa

La normativa, europea e nazionale, prevede che, in base alla finalità del trattamento, il titolare debba fornire agli interessati, prima del trattamento, le informazioni richieste dalle norme. Ciò avviene tramite l'**informativa**.
L'informativa è una comunicazione rivolta all'interessato finalizzata ad informarlo, così che possa rendere un valido consenso. Essa è condizione, non tanto del rispetto del diritto individuale ad essere informato, quanto del dovere del titolare del trattamento di garantire la lealtà del trattamento.
L'informativa può anche essere orale, ma è preferibile sia data per iscritto al fine di provarne l'esistenza e per consentire alle autorità di vigilanza di verificarne la completezza e correttezza.

Quando è dovuta
Se un sito web non permette alcuna registrazione degli utenti, e non tratta dati degli utenti, non occorre l'informativa privacy, anche se occorre tenere presente che i siti web in genere acquisiscono comunque informazioni tramite i server sui quali sono ospitati. Invece, **l'informativa è sempre dovuta ogni qual volta vi sia una raccolta e trattamento dei dati** (es. indirizzi IP, mail) degli utenti (es. compilazione moduli), per cui anche nel caso in cui il sito utilizzi cookie tramite i quali raccoglie dati degli utenti. E' altresì dovuta anche quando il consenso dell'interessato non è richiesto, oppure quando l'interessato è tenuto obbligatoriamente per legge a fornire i dati.
Se il sito permette la registrazione degli utenti, ma i dati vengono usati solo per fini del sito medesimo (es. mailing list) e non per l'invio di proposte commerciali ecc..., occorre solo l'informativa privacy (da linkare al modulo di registrazione per consentirne la consultazione), ma non occorre la raccolta del consenso.
Invece, se il sito permette la registrazione degli utenti e raccoglie dati anche a fini promozionali e pubblicitari, compreso la trasmissione a terzi, occorre l'informativa privacy e il consenso deve essere espresso con accettazione separata dell'informativa.

Contenuto minimo
L'informativa deve avere il seguente **contenuto minimo** (articoli 13 e 14 del Regolamento europeo):

- categorie di dati trattati e finalità del trattamento (non come vengono trattati i dati ma quali dati vengono trattati divisi per categorie, a quale fine, per quanto tempo sono trattati, se i dati verranno trasferiti all'estero e, in questo caso, attraverso quali strumenti);
- la **base giuridica** del trattamento, quindi se si tratta di trattamento basato su consenso o giustificato da leggi, legittimi interessi (in questo caso specificando quale è il legittimo interesse), ecc...;
- **natura obbligatoria o facoltativa del conferimento dei dati** (se il soggetto può rifiutare il consenso e le conseguenze di tale rifiuto, specificando che è possibile rifiutare il consenso a singoli trattamenti quali quelli a fini di marketing diretto);
- se il titolare ha intenzione di utilizzare i dati per una finalità diversa da quella per la quale sono stati raccolti;
- soggetti e categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi (l'indicazione di soggetti terzi non può essere generica);
- se il titolare ha intenzione di trasferire i dati in paesi extra UE;
- i diritti dell'interessato (diritto di chiedere se dati personali sono presenti nella banca dati, diritto di prenderne visione e di chiederne la modifica, diritto di presentare reclamo all'autorità di controllo, eventuale diritto alla portabilità) e in particolare il diritto di revocare il consenso in qualsiasi momento;
- **dati identificativi** (nome, denominazione o ragione sociale, domicilio o sede) del titolare del trattamento e, se designato, del responsabile per la protezione dei dati (DPO), quindi un recapito al quale gli interessati potranno rivolgersi per esercitare i propri diritti;
- se il trattamento comporta processi decisionali automatizzati (come la profilazione) deve essere specificato indicando anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

All'interno dell'informativa privacy devono essere indicati anche i cookie che veicola il sito, le modalità di disabilitazione dei cookie (es. tramite opzioni del browser), e nel caso di cookie di terze parti, il link alle pagine delle privacy policy dei servizi delle terze parti. Si rimanda ad altro articolo per ulteriori dettagli sulla regolamentazione dei cookie. Si fa presente che l'informativa cookie è una sezione dell'informativa privacy, non un documento separato, per cui generalmente si ammette che possa essere una pagina diversa da quella che contiene l'informativa privacy, ma quest'ultima deve assolutamente richiamarla (tramite link).

Modalità dell'informativa

L'informativa deve avere **forma coincisa, deve essere chiara, facilmente accessibile ed intellegibile** per l'interessato, eventualmente anche utilizzando immagini o icone (le icone devono essere identiche per tutta l'Unione europea e saranno identificate da un successivo provvedimento della Commissione europea).Va data preferibilmente per iscritto e in formato elettronico, ma sono ammessi anche altri mezzi, compreso la forma orale.
E' ammessa la possibilità di **pubblicare l'informativa su un sito web**, inserendo il collegamento (*link*) a tale pagina web nella pagina principale (*home*) del sito web, ma anche nelle comunicazioni e nella corrispondenza, compreso la corrispondenza cartacea. Nel caso di comunicazioni postali è, però, necessario prevedere anche delle forme alternative, come ad esempio l'invio di fax a seguito di richiesta da parte degli interessati, per coloro che non hanno la possibilità di leggerla online.
Nel caso in cui i **dati non siano raccolti direttamente presso l'interessato** (art. 14 del Regolamento), l'informativa deve essere fornita entro un termine ragionevole, e comunque non oltre 1 mese dalla raccolta dei dati. Oppure va fatta al momento della comunicazione dei dati a terzi. Comunque, in questo caso spetta al titolare valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato.
A tale proposito il Garante privacy italiano, ha ricordato che in alcuni casi non è necessaria l'informativa, quando:
- i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria (vedi basi giuridiche del trattamento);
- il trattamento è connesso allo svolgimento delle "investigazioni difensive" in materia penale (art. 38 norme di attuazione del c.p.p.) o alla difesa di un diritto in sede giudiziaria (a meno che il trattamento si protragga per un periodo superiore a quello strettamente necessario al perseguimento di tali finalità o sia svolto per ulteriori scopi).

Il Garante ha anche emanato alcuni provvedimenti in materia di esenzione all'informativa:
- Esonero dall'obbligo dell'informativa nel caso siano necessari mezzi manifestamente sproporzionati - 26 novembre 1998;
- Esonero per l'obbligo dell'informativa per il trattamento dei dati utilizzati nello svolgimento dell'attività d'impresa - 19 febbraio 2015.

Sanzioni
Una violazione in materia di informazione agli utenti può avere come conseguenza l'indagine da parte dell'autorità di controllo, la quale può imporre delle sanzioni e anche il blocco di tutti i dati raccolti ed elaborati in violazione delle norme.
Inoltre, gli utenti possono avviare una azione per il risarcimento dei danno contro il titolare del trattamento.

Tutela da trattamento illecito di dati personali

Il regolamento europeo per la protezione dei dati personali stabilisce che chiunque subisca un danno, materiale o immateriale, a seguito di un trattamento di dati non conforme al regolamento, ha il diritto di ottenere il risarcimento del danno subito.
L'articolo 82 del GDPR, quindi, stabilisce il diritto ad ottenere il **risarcimento del danno** da parte dell'interessato (e quindi danneggiato). I soggetti tenuti al risarcimento sono sia il titolare che il responsabile del trattamento. Il titolare risponde per il danno causato dal trattamento in violazione del regolamento, mentre il responsabile risponde del danno causato dal non corretto adempimento dei suoi obblighi specifici, o se ha agito in modo difforme rispetto alla istruzioni del titolare.
Ovviamente un trattamento non conforme alle norme, e quindi illecito, determina innanzitutto l'**impossibilità di utilizzare i dati raccolti**.
Per far valere i propri diritti, un cittadino, cioè l'interessato al trattamento, può utilizzare vari strumenti. Il Garante per la protezione dei dati personali ha predisposto delle FAQ in materia.

Interpello al titolare del trattamento
L'interessato al trattamento che ritiene di aver subito una violazione dei suoi diritti può rivolgersi direttamente al titolare del trattamento (o al responsabile o anche attraverso un incaricato) per la sua tutela, senza particolari formalità (per lettera, mail, fax, ecc...). Un classico esempio è la richiesta di diritto all'oblio (cancellazione) che può essere rivolta direttamente a Google Search (e agli altri motori di ricerca) quale titolare del trattamento.
L'interessato deve ricevere una risposta entro 15 giorni, termine che può essere esteso a 30 giorni, dandone comunicazione all'interessato nei primi 15 giorni.
In mancanza di risposta, o in caso di risposta non soddisfacente, l'interessato può rivolgersi all'Autorità di controllo (Garante) o a quella giudiziaria.
QUI il modello per l'interpello al titolare, predisposto dal Garante

Tutela amministrativa
L'articolo 141 del codice per la protezione dei dati personali prevede la possibilità di rivolgersi anche al Garante per la tutela dei propri diritti, in alternativa al giudice ordinario (cioè dopo essersi rivolti al Garante non è più ammissibile rivolgersi al giudice ordinario, se non nel caso del ricorso), direttamente oppure a seguito di non accoglimento della richiesta rivolta al titolare del trattamento.

Reclamo
L'interessato può presentare un **reclamo** al Garante, col quale rappresenta una violazione della normativa in materia di protezione dei dati personali. Il reclamo, regolamentato dall'articolo 142 del codice, deve contenere una serie di elementi, in particolare l'indicazione dettagliata dei fatti e delle circostanze, delle norme che si presumono violate e delle misure richieste. Per la presentazione del reclamo occorre pagare i diritti di segretaria (150 euro).
Al termine del procedimento amministrativo, il Garante emana un provvedimento col quale l'autorità può prescrivere le misure per rendere il trattamento conforme alle disposizioni di legge, oppure intimare il blocco o il divieto del trattamento che risulti illecito o non corretto.

Segnalazione
La **segnalazione** è un atto col quale si sollecita al Garante (qui i contatti) un controllo sull'applicazione della normativa in relazione ad un trattamento. Non richiede il pagamento di diritti di segreteria, né una descrizione dettagliata dei fatti, ma deve contenere gli elementi utili per l'intervento del Garante. In sostanza si sostituisce al reclamo nel caso in cui non si abbiano elementi circostanziati.
Al seguito dell'eventuale istruttoria, il Garante può emanare gli stessi provvedimenti di cui al reclamo.

Ricorso
Il **ricorso**, invece, è un **atto formale che può essere presentato solo per far valere i diritti di cui all'articolo 7 del codice per la protezione dei dati personali** (qui il FAQ del Garante). Il ricorso può essere presentato se l'istanza con la quale l'interessato esercita tali diritti non riceve risposta nei tempi previsti (cioè 15 gioni dal ricevimento, oppure 30 giorni nei casi più complessi, previo avvertimento all'istante) dal titolare del trattamento, se la risposta non è soddisfacente, oppure se il decorso dei termini può esporre l'interessato ad un pregiudizio irreparabile. Per presentare il ricorso occorre pagare i diritti di segreteria (150 euro), e deve contenere gli elementi prescritti dall'articolo 147 del codice. Il ricorso non può essere proposto se è già stata adita l'autorità giudiziaria.

Il Garante può, in via provvisoria, disporre il blocco del trattamento, in tutto o in parte. A seguito del procedimento amministrativo emana un provvedimento col quale ordina la cessazione del trattamento illecito, indicando le misure necessarie a tutela dell'interessato. La mancata pronuncia nel termine di 60 giorni equivale a rigetto del ricorso.
Se l'interessato lo ha richiesto, il Garante condanna l'altra parte al ristoro delle spese sostenute per la presentazione del ricorso (nella pressi vanno da 500 a 1.000 euro), condanna che in assenza di opposizione diventa titolo esecutivo. Il Garante, invece, non ha competenza per decidere sui danni.
Contro il provvedimento (anche in caso di mancata pronuncia nei 60 giorni) può essere proposta **opposizione all'autorità giudiziaria**.

Tutela civile
L'interessato in alternativa al ricorso al Garante può rivolgersi anche al giudice civile, e in particolare al tribunale del luogo di residenza del titolare del trattamento. Può anche presentare opposizione al provvedimento che conclude il procedimento di ricorso.
Solo il tribunale può condannare il titolare del trattamento illecito al **risarcimento dei danni** occorsi all'interessato. L'art. 13 del Codice Privacy prevede espressamente che chiunque cagiona un danno ad altri, per effetto del trattamento di dati personali, è tenuto al risarcimento del danno ai sensi dell'art. 2050 del codice civile. L'art. 2050 riguarda i casi di **responsabilità per l'esercizio di attività pericolose**. Il richiamo di tale articolo evidenzia che l'interessato che ha subito un danno potrà limitarsi a dimostrare l'esistenza del danno e che esso è conseguenza del trattamento illecito, mentre spetta al titolare del trattamento, casomai in solido col responsabile, dimostrare di aver adottato tutte le misure idonee per evitare il danno.
Ovviamente, il danno non può identificarsi nell'evento dannoso (cioé l'illecito trattamento dei dati) ma é necessario che si concreti un un pregiudizio della sfera non patrimoniale di interessi del danneggiato.

Provvedimenti di urgenza
In casi di urgenza è possibile ricorrere all'art. 700 c.p.c. In questo caso occorre provare il *fumus boni iuris* (cioè che la pretese non sia infondata o temeraria) e il *periculum in mora* (pericolo che nel tempo necessario ad ottenere una pronuncia giudiziale possano intervenire fatti irreparabili che impedirebbero l'applicazione di un eventuale giudizio favorevole). Quest'ultimo si ritiene sempre sussistente in caso di pubblicazione online, dato la permanenza e quindi della lesione continuata del diritto.
Se sussiste anche una violazione del diritto di immagine si può ricorrere alla tutela d'urgenza prevista dalla legge sul diritto d'autore (articoli 96 e seguenti).

Tutela penale
La responsabilità penale, invece, è regolamentata dall'art. 167 del codice privacy (si fa presente che lo schema di decreto per l'attuazione del GDPR in Italia prevederebbe l'abrogazione di tale norma penale). Tale articolo sanziona diversi tipi di condotte.
Il trattamento illecito dei dati, per essere penalmente perseguibile deve essere caratterizzato dal **dolo specifico**, cioè chi pone in essere la condotta deve agire al fine di trarre per sé o per altri un profitto, ovvero per recare ad altri un pregiudizio, e comportare altresì la produzione di un nocumento, che è prevista quale condizione obiettiva di punibilità.
Di conseguenza anche se il trattamento dei dati è avvenuto senza il consenso dell'interessato, non è punibile a meno che non abbia prodotto un danno.

Consenso al trattamento

Il consenso è una delle basi giuridiche del trattamento, nell'ambito del regolamento generale per la protezione dei dati personali.

Definizione
Il **consenso,** in base al nuovo Regolamento Generale (art. 4 GDPR), è qualsiasi **manifestazione di volontà libera, specifica, informata e inequivocabile** dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. Il presupposto indefettibile è che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo.
In caso di trattamento di dati di minori, occorre acquisire il consenso dai genitori o dagli esercenti la patria potestà se l'interessato ha meno di 16 anni.
Inoltre, in base al Considerando 32: "*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. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso*".

Caratteristiche
Il consenso deve essere:
1) inequivocabile;
2) libero;
3) specifico;
4) informato;
5) verificabile;
6) revocabile.
1) Consenso **inequivocabile** (*unambiguous* nella versione inglese) vuol dire che non è necessario che sia esplicito ma **può anche essere implicito** (ma non tacito), purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso (es. l'inerzia non può costituire manifestazione di consenso, come anche i form precompilati e caselle già prespuntate). Cioè deve prevedere una chiara azione positiva (come spuntare una casella od inserire la mail in un campo dove è specificata la finalità per la quale sarà usato il dato).
Il consenso deve, invece, essere **esplicito** (art. 9 GDPR) nel caso di trattamento di dati sensibili o nel caso di **processi decisionali automatizzati** (es. profilazione).
Occorre dire che la versione originaria della proposta della Commissione europea prevedeva sempre il consenso esplicito, poi si è pervenuti al compromesso attuale.

2) Il consenso deve essere dato **liberamente**, il ché significa che l'interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso. L'articolo 7 del GDPR chiarisce 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*".
Ad esempio, nel caso di pubblicità commerciale, **il consenso deve essere separato rispetto al consenso per la prestazione contrattuale richiesta dall'utente**, perchè l'utente deve avere la possibilità di addivenire al contratto senza dover subire il ricatto di dover ricevere pubblicità commerciale. Non può definirsi libero il consenso a ulteriori trattamenti dei dati personali che l'interessato debba prestare quale condizione per conseguire una prestazione richiesta (provvedimento del Garante del 31 gennaio 2008).

Questo purtroppo porta al rischio che molti dei consensi ottenuti dai servizi online possano essere ritenuti invalidi. Lo stesso Gruppo Articolo 29 fornisce un esempio chiarificatore: una app mobile per il fotoritocco chiede il consenso per accedere alla geolocalizzazione e i dati vengono utilizzati a fini di pubblicità comportamentale. Ma né la

geolocalizzazione, né la pubblicità sono necessari per la fornitura del servizio (fotoritocco), per cui subordinare l'uso della App a tale consenso rende il consenso non libero e quindi illecito.
Un altro problema riguarda il **consenso dei dipendenti**. Se il datore di lavoro richiede il consenso all'utilizzo del dato (es. vuole pubblicare la foto dei dipendenti sul sito web aziendale) e vi è un pregiudizio reale o potenziale per il cliente non consenziente (cosa altamente probabile in un contesto lavorativo), il consenso non può ritenersi valido perché non libero. Dato lo squilibrio di potere tra datore e dipendente, quest'ultimo può dare un consenso valido solo in circostanze eccezionali. Quindi, il consenso non può costituire la base giuridica del trattamento in caso di **evidente squilibrio tra le parti**. In tal caso sarebbe preferibile trattare i dati su base giuridica differente.

3) Il consenso deve essere **specifico**, cioè relativo alla finalità per la quale è eseguito quel trattamento. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità (Considerando 32 GDPR). Quindi, i dati dovranno essere pertinenti al consenso fornito, e in caso di modifiche del trattamento occorre richiedere un nuovo consenso. Per cui avremo un consenso per il marketing diretto, un consenso per la profilazione, ecc...

4) Il consenso deve essere **informato**, occorre cioè che l'interessato sia posto in condizioni di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge. Inoltre l'interessato deve essere opportunamente informato sulle conseguenze del suo consenso (ad esempio deve essere indicato che in assenza di consenso non potrà accedere a determinate sezioni del sito web). L'informazione si ha attraverso l'apposita informativa. Il regolamento europeo si concreta, più che sui requisiti formali del consenso, sulla necessità della validità sostanziale del consenso, per cui l'aspetto informativo è essenziale, richiedendo un linguaggio semplice e comprensibile, anche eventualmente colloquiale.

5) Consenso **verificabile** non vuol dire che il consenso deve essere documentato per iscritto, né che è richiesta la forma scritta (anche se in alcune ipotesi -es. dati sensibili- può essere preferibile perché consente più facilmente di provare il consenso, facilitando quindi le verifiche da parte dell'autorità), ma che l'azienda deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento (quindi distinguendo tra i vari trattamenti). L'azienda dovrà essere in grado di sapere anche a quale informativa l'utente ha acconsentito, distinguendo tra le varie versioni.
Il WP29 suggerisce di utilizzare un registro nel quale siano conservate le informazioni relative alla sessione in cui è stato espresso il consenso, unitamente alla documentazione del flusso di lavoro del consenso, e una copia delle informazioni presentate all'interessato in quel momento.

6) Il consenso **deve essere revocabile** in qualsiasi momento. La revoca deve essere facile così come lo è dare il consenso. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi (ovviamente la revoca non comporta illiceità del trattamento precedente, ma solo l'obbligo di terminare il trattamento), a meno che non sussista una differente base giuridica per continuare il trattamento.
Per revocare il consenso, quindi, il titolare dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso. In alternativa è possibile revocare il consenso inviando una comunicazione, o tramite un apposito form sul sito, o tramite mail, ai contatti indicati nel sito all'interno dell'informativa (interpello al titolare). Nel caso in cui il titolare non ottemperi, ci si può rivolgere al Garante o al tribunale per la tutela dei propri diritti.
Con la revoca si innesca il diritto di cancellazione, per cui l'azienda deve cancellare i dati dell'utente. Ovviamente vi sono motivi legittimi in base ai quali un'azienda ha necessità di conservare alcuni dati dell'utente anche dopo la revoca del consenso, come ad esempio mantenere un registro delle transazioni per motivi fiscali. In ogni caso l'azienda può avvertire l'interessato che a seguito della revoca del consenso, vi sarà la cancellazione dei dati è la conseguente impossibilità di fornire ulteriori servizi.

Scadenza
Occorre tenere presente che il consenso non dura per sempre. Quando si raccolgono dati personali occorre informare l'interessato della **durata della conservazione (e quindi trattamento) del dato**, scaduta la quale il dato va o anonimizzato oppure cancellato. Per questo motivo in alcuni casi potrebbe essere preferibile una base giuridica diversa dal consenso, come ad esempio i legittimi interessi del titolare del trattamento.

Dati sensibili
Il consenso è l'unica base giuridica utile per il trattamento dei dati sensibili, nel qual caso deve essere esplicito. A parte il trattamento per l'attività giornalistica, che è a forma libera per qualsiasi tipo di dato.

Dato Personale

Il **dato personale** rappresenta lo strumento tecnico-giuridico attraverso il quale i legislatori, nazionali e comunitari, tutelano l'insieme dei diritti collegati all'identità personale, quindi è un bene giuridico di secondo grado.
Dato personale è qualsiasi informazione (nome, codice fiscale, immagine, voce, impronta digitale, traffico telefonico) concernente una **persona fisica identificata o identificabile**, anche indirettamente, oppure informazioni riguardanti una persona la cui identità è nota o può comunque essere accertata mediante informazioni suplementari (Convenzione 108, art. 2, lett. a) e Direttiva sulla protezione dei dati, articolo. 2, lett. a)). La persona a cui si riferiscono i dati soggetti al trattamento si definisce "interessato".

Identificazione
Identificabile è la persona che può essere identificata direttamente o indirettamente, anche mediante il riferimento ad ulteriori elementi. Per **identificazione**, quindi, si deve intendere la possibilità di distinguere la persona da qualsiasi altro soggetto (es. qualifica di presidente del consiglio) oppure all'interno di una categoria. Se l'identificazione richiede l'acquisizione di ulteriori dati per i quali occorrono tempi e costi irragionevoli, allora la persona non si può considerare identificabile. In ogni caso non è necessario raggiungere un elevato livello di identificazione (pensiamo ai nomi che corrispondono a più persone) perchè il dato sia assoggettato a tutela.
I dati si considerano personali **se consentono l'identificazione** dell'individuo oppure se le informazioni **descrivono l'individuo** in modo tale da consentirne l'identificazione acquisendo altri dati. Entrambi i tipi di dati sono tutelati allo stesso modo.

Quindi **il dato personale è un concetto dinamico, che va sempre riferito al contesto**, nel senso che anche se un'informazione isolata non è in grado di portare all'identificazione di un individuo, il fatto che detta informazione possa essere utilizzata per l'identificazione tramite incrocio con altri dati ne determina la natura di dato personale.
Non occorre, inoltre, che l'informazione sia in grado di individuare fisicamente la persona per essere considerata dato personale. Ad esempio, le aziende di pubblicità utilizzano vari tecniche di tracciamento per poter identificare singolarmente un individuo tra i tanti navigatori online, dette tecniche non permettono l'individuazione fisica della persona ma più che altro identificano il browser o il dispositivo digitale tramite il quale la persona naviga in rete.
Anche questi dati (cookie, fingerprint, adid) sono considerati dati personali.

Il criterio dell'**identificabilità mediante incrocio di informazioni**, anche se detenute da diversi titolari, fa sì che anche i dati online, come i numeri IP e i cookie rientrino nel concetto di dato personale. La Corte di Giustizia europea ha espressamente definito l'indirizzo IP (Internet Protocol) come dato personale, anche con riferimento all'IP dinamico (sentenza Breyer contro Germania del 2016). L'account di un servizio online è sicuramente un dato personale, in quanto consente di identificare univocamente una persona, così come la mail, il nickname. Il fatto che l'IP sia considerato dato personale impedisce ad una azienda di ottenere dall'ISP (fornitore di accesso ad Internet) il nominativo di un soggetto che ha scaricato file piratati online. Solo l'autorità giudiziaria può, infatti, può accedere a tali informazioni.
Il nuovo Regolamento europeo in materia di tutela dei dati personali (General Data Protection Regulation) include espressamente nei dati personali gli identificatori online, quali numeri IP, cookie e dati di geolocalizzazione.
Esempi di dati personali sono: voce, immagini, filmati, fotografie, numero di telefono, codice fiscale, targa automobilistica, impronta digitale, ore di servizio prestate da un dipendente, informazioni sul comportamento di un lavoratore, informazioni sulle condizioni patrimoniali.
La Corte dei diritti dell'uomo ha evidenziato che non esiste una netta separazione tra **vita privata e vita professionale** per quanto riguarda i dati personali, per cui anche le informazioni riguardanti la vita professionale e pubblica di una persona sono dati personali.
In tal senso si potrebbe ritenere che i diritti della CEDU appartengano non solo alle **persone fisiche** ma anche alle **persone giuridiche**. Per queste ultime la Corte dei diritti dell'uomo tende a considerare più che altro il diritto al rispetto del "domicilio" e della "corrispondenza". In realtà la Convenzione 108 consente alle parti contraenti di estendere la tutela prevista per le persone fisiche anche alle persone giuridiche. Il diritto dell'Unione europea, comunque, non contempla norme a tutela dei dati personali delle persone giuridiche, e nemmeno la normativa italiana.

Il **formato** (immagini, suoni, ecc...) nel quale sono conservati i dati è irrilevanti al fini dell'applicabilità della tutela dei dati personali.

Categorie di dati

Dati identificativi

Le informazioni di identificazione personale (**PII, Personally identifiable information**) sono dati che consentono l'identificazione diretta dell'interessato. Secondo la definizione utilizzata dall'Istituto nazionale degli standard e della tecnologia (NIST) tra tali dati ci sono:

- nome e cognome
- indirizzo di casa
- indirizzo email
- numero identificativo nazionale
- numero di passaporto
- indirizzo IP (quando collegato ad altri datii)
- numero di targa del veicolo
- numero di patente
- volto, impronte digitali o calligrafia
- numeri di carta di credito
- identità digitale
- data di nascita
- luogo di nascita
- informazioni genetiche
- numero di telefono
- account name o nickname.

Dati soggetti a trattamento speciale (dati sensibili)

L'articolo 9 del GDPR sancisce un generale divieto di trattare dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute (anche la semplice ferita ad una mano) o alla vita sessuale o all'orientamento sessuale della persona.
Col nuovo regolamento europeo, quindi, non si parla più di "dati sensibili", ma di **dati soggetti a trattamento speciale**. Sono quei dati la cui tutela ha lo scopo di garantire la libertà di pensiero e di opinione, la dignità della persona e la libertà da possibili discriminazioni. Per i dati sensibili già Convenzione 108 prevede una tutela rafforzata, cioè si prescrive il consenso esplicito, anche se non necessariamente scritto, perché riguardano aspetti particolarmente privati dell'individuo e possono essere usati a fini discriminatori. Rispetto alla precedente normativa, il regolamento europeo introduce anche i **dati genetici** tra quelli a trattamento speciale, nonché i **dati biometrici** (es. un gruppo di fotografie caricate online) se utilizzati per identificare in modo univoco una persona (ad esempio negli aeroporti dove l'immagine dell'individuo viene scansionata per identificarlo). Anche i dati **giudiziari** sono considerati dati sottoposti a trattamento speciale e sono quei dati che rivelano l'esistenza di provvedimenti penali suscettibili di iscrizione nel casellario giudiziale, o la qualità di indagato o imputato.
Questo tipo di dati possono essere trattati solo nei casi espressamente indicati:

- l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di **diritto del lavoro e della sicurezza sociale e protezione sociale**, nella misura in cui sia autorizzato da norme giuridiche o contratti collettivi;
- il trattamento è necessario per **tutelare un interesse vitale dell'interessato o di un'altra persona fisica** (vedi basi giuridiche del trattamento), qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento è effettuato da una **fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali**, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
- il trattamento riguarda **dati personali resi manifestamente pubblici dall'interessato**;
- il trattamento è necessario per **accertare, esercitare o difendere un diritto in sede giudiziaria** o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento è necessario per **motivi di interesse pubblico rilevante** sulla base di norme giuridiche, prevedendo misure appropriate per tutelare i diritti dell'interessato;
- il trattamento è necessario per **finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;

- il trattamento è necessario per **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti dell'interessato, in particolare il segreto professionale;
- il trattamento è necessario a f**ini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici**.

Inoltre, i dati personali di cui all'articolo 9 del GDPR possono essere trattati se il **trattamento avviene ad opera o sotto la responsabilità di un professionista soggetto al segreto professionale** conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.
Per la qualificazione di un dato come soggetto a trattamento speciale, è importante tenere presente il contesto. Ad esempio, l'immagine di un individuo che indossa abiti religiosi non è considerata dato soggetto a trattamento speciale, in quanto l'individuo in questione esercita la sua professione, così come non lo è l'immagine di un politico ritratta col simbolo del partito. Invece, l'immagine di una persona che entra in un luogo di culto o in una sede di partito è dato soggetto a trattamento speciale in quanto è indice della scelta effettuata.

Dati anonimi, pseudonimi, e minimizzazione

La Convenzione 108 e il regolamento europeo prevedono che i dati devono essere conservati per un periodo di tempo limitato, e in particolare non oltre il tempo necessario per raggiungere lo scopo alla base del trattamento. Nel caso in cui un titolare del trattamento volesse mantenerli per un periodo superiore, deve procedere alla loro anonimizzazione.

Dati anonimizzati sono quei dati che sono stati privati di tutti gli elementi identificativi. I dati anonimizzati non sono ritenuti dati personali, e quindi non sono soggetti alle norme a tutela dei dati personali.
Ovviamente può accadere che i dati, una volta esaurito lo scopo del trattamento, debbano comunque essere conservati a fini statistici, storici o scientifici. In questo caso occorre che siano applicate adeguate misure contro possibili abusi dei dati.

Dati pseudonimi sono quei dati personali nei quali gli elementi identificativi sono stati sostituiti da elementi diversi, quali stringhe di caratteri o numeri (*hash*), oppure sostituendo al nome un nickname, purché sia tale da rendere estremamente difficoltosa l'identificazione dell'interessato. Ovviamente il soggetto che detiene la chiave per decifrare i dati (cioè collegare l'elemento pseudonimo al dato personale) deve garantire adeguate misure contro possibili abusi.
I dati pseudonimi, a differenza di quelli anonimizzati, sono comunque dati personali (in quanto consentono l'identificazione della persona, anche se indirettamente, tramite incrocio con altre informazioni), anche se soggetti ad una tutela ridotta rispetto ai dati personali veri e propri. Ad esempio, l'articolo 33 del GDPR precisa che il titolare del trattamento deve notificare al Garante una violazione dei dati personali, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Se la pseudonimizzazione è avvenuta in modo sicuro un rischio è improbabile. Inoltre, **le aziende possono creare profili a fini di marketing anche senza il consenso degli interessati, purché i dati rimangano pseudonimi.**
In ogni caso il titolare del trattamento che, invece di evitare l'uso di dati personali, adopera dati pseudo-anonimi deve spiegare agli interessati la logica e le motivazioni per tale scelta.
La **minimizzazione**, invece, consiste nella raccolta dei soli dati pertinenti, quindi limitando il trattamento a ciò che è realmente necessario e indispensabile rispetto alla finalità alla quale sono destinati. La minimizzazione in realtà è da considerarsi un vero e proprio principio fondamentale (principio di pertinenza dei dati) che regolamenta il trattamento dei dati personali, perché nell'ordinamento europeo il trattamento deve sempre essere limitato ai soli dati strettamente necessari.

GDPR

Ciclo del dato personale

Tipo dati raccolti

Raccogli troppi dati personali per raggiungere gli scopi prefissi?
Puoi ridurre il numero di dati raccolti ottenendo gli stessi risultati?

Finalità della raccolta

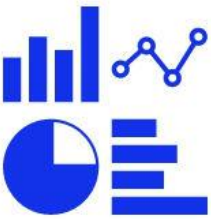
Quale è lo scopo della raccolta dei dati?
Lo hai specificato nell'informativa? Lo hai comunicato agli interessati?
Gli interessati sono a conoscenza di cosa accade ai loro dati quando te li conferiscono?

Aggiornamento dei dati

Hai una procedura per la verifica dell'esattezza dei dati e il loro eventuale aggiornamento?

Conservazione dei dati

Hai adottato misure per la sicurezza dei dati?
Ai dati possono accedere solo le persone autorizzate?
Hai adottato misure di backup dei dati?
Se il backup è nel Cloud, il fornitore del servizio è in regola con le norme?



Tempo di conservazione dei dati

Per quanto tempo i dati vengono conservati?
Hai procedure per la verifica che i dati siano conservati solo per il periodo necessario a raggiungere gli scopi prefissati?

Diritti dell'interessato

Garantisci i diritti all'interessato (diritto di accesso, cancellazione e portabilità)?
Rispondi alle richieste dell'interessato nei tempi previsti dalle norme?

Tutela dei dati personali di minori

La tutela dei dati personali e della privacy dei **minori** è divenuta un problema rilevante con l'avvento dei social network. La minore età, infatti, è legata a diritti rafforzati rispetto agli adulti, per cui il trattamento da parte delle aziende dei loro dati deve essere regolamentato in maniera differente.

Minori e social network

Regolamentazione attuale

I principali social network prevedono una età minima per iscriversi fissata a **13 anni:**

– Facebook: 13 anni
– Instagram: 13 anni
– Whatsapp: 13 anni (prima era 16 anni);
– Snapchat: 13 anni;
- Youtube 13 anni.

Questo perché le principali piattaforme online sono americane, e quindi applicano il limite fissato dalla legge federale Usa: il Children's Online Privacy Protection Act (**COPPA**). Tale legge prescrive che nessuna persona giuridica (tranne gli enti pubblici) può raccogliere dati relativi a minori di 13 anni. Il COPPA prevede, inoltre, il preavviso di trattamento ai genitori, il consenso degli stessi, dimostrabile a richiesta, l'obbligo di adottare misure di sicurezza e il divieto di sollecitare dati non necessari al trattamento.
Generalmente i social network prevedono un apposito modulo (qui quello di Facebook) per comunicare account di persone con età inferiore a quella consentita, nel qual caso provvedono a rimuovere l'account.
L'**attuale normativa europea**, invece, non prevede un vero e proprio limite che, però, è ricavabile dal quadro normativo generale. In Italia, ad esempio, la capacità di agire si acquista con la maggiore età, quindi a 18 anni. Il minore con età compresa tra 14 e 18 ha una capacità giuridica attenuata, il minore dei 14 anni non è imputabile e non ha capacità giuridica. Come esempio, consideriamo che la normativa europea prevede espressamente che solo a 16 anni un soggetto può dare autonomamente il proprio consenso al trattamento medico, mentre al di sotto dei 16 anni il medico dovrebbe valutare il grado di maturità del minore per verificare se è in grado di prendere decisioni autonome, oppure raccogliere il consenso di un genitore o tutore.
L'adolescente (minore tra i 16 e i 18 anni non soggetto ad obbligo scolastico) ha una capacità giuridica attenuata, può sottoscrivere un contratto (come quello di iscrizione ad un social), ma non dovrebbe poter acconsentire ad atti che richiedono un consenso libero, specifico ed informato, come è la profilazione.
Il Garante spagnolo ha invece fissato l'età a 14, nel rispetto della normativa nazionale che consente solo a chi ha compiuto i 14 anni di diffondere in rete i propri dati personali, condividendoli con altri.

Regolamentazione europea dal 25 maggio 2018

Il nuovo Regolamento europeo (GDPR) ha, invece, prescritto, all'articolo 8, l'obbligo di **non consentire l'offerta diretta di servizi della società dell'informazione (quindi iscrizione ai social network e ai servizi di messagistica) a soggetti minori di 16 anni**, a meno che non sia raccolto il consenso dei genitori (occorre accertare che il consenso sia dato dall'esercente la patria potestà) o di chi ne fa le veci. La norma prevede, però, che questo aspetto possa essere regolato diversamente dagli Stati nazionali (ma il limite non può scendere al di sotto dei 13 anni). In tale prospettiva **il legislatore italiano ha proposto di fissare il limite di età da applicare in Italia in 16 anni** (la normativa è ancora in discussione, quindi può essere modificata).

Occorre tenere presente che l'iscrizione ad un servizio online come, ad esempio, Facebook, non è più, non solo, l'iscrizione al social ma un vero e proprio contratto con quale l'utente consente ad una profilazione spinta dei propri comportamenti. L'iscrizione ad un social network o in genere ad un servizio online, quindi, è assoggettata alle regole per la conclusione dei contratti, per i quali occorre che il soggetto sia in grado di apprezzare la natura e le conseguenze del suo consenso.
In ogni caso, il **consenso dei genitori** non è sempre necessario. In base all'articolo 8 del nuovo regolamento europeo il consenso dei genitori è richiesto solo se il trattamento dei dati dei minori è legittimato sulla base del consenso. Se, invece, il trattamento ha altra base giuridica, come ad esempio il rispetto di un obbligo di legge, i legittimi interessi, ecc..., il consenso dei genitori non è necessario.

Minori e cronaca

L'attuale normativa prevede un generale principio di preminenza dell'interesse del minore, il quale comporta delle limitazioni nel trattamento dei dati personali anche da parte dei giornalisti, il cui trattamento normalmente è

svincolato da limiti. Fermo restando che la valutazione dell'interesse pubblico alla pubblicazione dei dati dei minori va attuata dal giornalista, questi ha comunque l'obbligo di non pubblicare informazioni o immagini del minore se non nell'interesse oggettivo del minore stesso, e di astenersi dalla pubblicazione di informazioni in grado di consentire l'identificazione del minore stesso, anche a livello locale. Intendendosi che si deve far riferimento anche ad una identificazione indiretta (ad esempio, la pubblicazione di dati o informazioni di genitori, parenti, amici, ecc...).

Adozioni

La notizia che un minore è in stato di adozione non si può pubblicare a meno che non vi sia l'espresso consenso dei genitori. Con riferimento ai bambini adottati, infatti, non solo si deve considerare la normativa in materia di protezione dei dati, ma anche quella specifica in materia di adozione, che prevede l'affidamento ai genitori della scelta sui modi e i termini per informare il minore del suo stato di adottato.
La normativa (legge 4 maggio 1983) disciplina altresì i presupposti perché l'adottato possa accedere alle informazioni sulla sua origine e i suoi genitori biologici. Per cui è vietato anche diffondere, con riferimento a storie di figli adottivi, i dati reali e le informazioni idonee a permettere l'identificazione dei genitori reali.

Cyberbullismo

La recente legge 71 del 2017 ha previsto degli specifici compiti da parte dell'Autorità Garante per la Privacy in materia di cyberbullismo. La legge prevede misure di prevenzione ed educazione nelle scuole, sia per la vittime che per gli autori di atti di cyberbullismo. Inoltre, i minori potranno chiedere l'oscuramento o la rimozione di contenuti offensivi senza dover informare i propri genitori. La richiesta va inoltrata al gestore del sito o al titolare del trattamento, e, in seconda battuta (questa volta a mezzo dei genitori), al Garante, che interverrà in 48 ore.
-> modello per la segnalazione di atti di cyberbullismo

Pubblicazione di fotografie online

La pubblicazione di una fotografia online si inquadra pacificamente nel trattamento di dati personali e sensibili, e costituisce interferenza nella vita privata del minore. In tal senso occorre fare particolare attenzione nel pubblicare immagini di minori, anche se si tratta dei propri figli.
In quest'ottica una recente sentenza del tribunale di Mantova (novembre 2017) ha stabilito che per la pubblicazione delle foto dei figli occorre il consenso di entrambi i genitori. In assenza dell'accordo dei due genitori, la foto non è pubblicabile. Nel caso specifico il giudice Berardi ha, infatti, sostenuto che la pubblicazione delle immagini da parte della madre ma in assenza di consenso del padre, viola l'articolo 10 del codice civile in tema di diritto all'immagine, viola gli articoli 4,7,8 e 145 del d. lgs. 30 giugno 2003 n. 196 (Codice Privacy) riguardanti la tutela della riservatezza dei dati personali e anche gli articoli 1 e 16, I comma, della Convenzione di New York del 20/11/1989 sui diritto del fanciullo, ratificata dall'Italia con legge 27 maggio 1991 n. 176.

Scuola

Anche le istituzioni scolastiche, durante lo svolgimento dei loro compiti, hanno il dovere di rispettare la privacy e tutelare e proteggere i dati personali che trattano, in particolare perchè si tratta di soggetti spesso minorenni.
Le scuole, quindi, sia pubbliche che private, hanno l'obbligo di informare (tramite apposita informativa) gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Si intende che gli interessati non sono solo gli studenti, ma anche le famiglie, e gli stessi professori.
E' altresì importante che le scuole verifichino i loro trattamenti controllando se i dati siano eccedenti rispetto alle finalità perseguite.

Scuole pubbliche
Le istituzioni scolastiche pubbliche possono trattare soltanto i dati personali necessari al perseguimento delle specifiche finalità istituzionali, che sono comunque **finalità di rilevante interesse pubblico**, in ossequio ai principi di finalità e non eccedenza, oppure quelli espressamente previsti dalla normativa di settore. Non possono essere chiesti dati non rilevanti per la finalità istituzionali. Quindi, per tali trattamenti non occorre il consenso degli studenti, la base giuridica del trattamento è, infatti, data dall'interesse pubblico.
Occorre, ovviamente, particolare cautela nel trattamento dei dati, trattandosi di dati relativi a soggetti generalmente minorenni. In alcuni casi si tratta anche di dati sensibili, dati cioè relativi alla salute o dati giudiziari. In questo caso le cautele devono essere massime e soprattutto occorre verificare se il trattamento di quei dati sia davvero necessario per il perseguimento delle finalità scolastiche.

Scuole private
Nelle scuole private la base legale per il trattamento è data dal **consenso dell'interessato**, da intendersi, ovviamente, il genitore o chi esercita la tutela, nel caso di minori.
Le norme in materia di protezione dei dati personali, e in particolare il Codice della privacy, prevedono che **non sia necessario il consenso in tutti quei casi in cui il trattamento è previsto per legge o per l'adempimento di in contratto**, per cui in casi specifici, come relativamente ai dati per l'iscrizione a scuola o per specifiche attività scolastiche, non necessita il consenso degli interessati. Di contro occorrerà il consenso per tutte le attività non strettamente connesse a quelle didattiche.
Le istituzioni scolastiche private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli alunni, dati relativi alle convinzioni religiose al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli alunni.
Questi dati possono essere trattati anche in caso di contenziosi con alunni e genitori, al fine di difendere l'istituzione scolastica.

Accesso ai dati
Per conosce le informazioni e i dati eventualmente conservati dall'istituzione scolastica, ed esercitare i diritti di rettifica e correzione, è possibile rivolgersi al titolare del trattamento, in genere lo stesso istituto scolastico. In caso di mancata risposta ci si può rivolgere al Garante oppure alla magistratura. Per quanto riguarda, invece, i singoli atti amministrativi, spetta all'istituto valutare se il richiedente ha un interesse diretto, concreto ad attuale ad ottonere l'atto, in questione, in base alla legge 241 del 1990 che regola l'accesso agli atti della Pubblica Amministrazione.

Il Garante per la privacy ha pubblicato una esaustiva guida nel quale, oltre a chiarire la regolamentazione in materia, inserisce numerosi esempi pratici per comprendere come tutelare la privacy degli studenti (link alla guida).

Sanità

La riservatezza deve essere garantita in particolar modo per i cittadini che entrano in contatto con strutture sanitarie. I **dati sanitari**, infatti, sono considerati dati sensibili in quanto in grado di rivelare dettagli molto intimi della persona, e per questo vi è un generale divieto di trattamento e diffusione, nonché una tutela rafforzata, di tali dati.

Dati sanitari
I dati sanitari sono tutte quelle informazioni personali idonee a rivelare lo stato di salute, la vita sessuale e le condizioni corporee e mentali di una persona. Sono considerati dati sanitari anche i **dati genetici**, e le fotografie scattate a fini di interventi chirurgici.
Tali dati sono soggetti ad una tutela rafforzata e particolari cautele, come il divieto di diffusione. Inoltre, come stabilito dalla Cassazione (Cassazione Civile, SS.UU., sentenza 27/12/2017 n° 30981) i dati sensibili idonei a rivelare lo stato di salute devono essere trattati con modalità organizzative tali da tutelarli, come ad esempio tecniche di **cifratura** che rendono non identificabile l'interessato.
La tutela del singolo viene, però, ridotta nel momento in cui occorre bilanciarla con la tutela della collettività. Il regolamento europeo prevede che i dati sanitari possono essere utilizzati solo per finalità connesse alla salute (finalità di cura), per la supervisione del Sistema Sanitario Nazionale (finalità di governo) e per la ricerca nel pubblico interesse. Di contro lascia agli Stati la possibilità di introdurre condizioni particolari o ulteriori limiti per il trattamento.

Trattamento, soggetti e base giuridica
Il trattamento dei dati sanitari è soggetto ad una disciplina specifica. Il trattamento dei dati sanitari può essere effettuato da:
- esercenti una professione sanitaria (sono esclusi gli ortopedici, gli igienisti dentali, infermieri, ostetrici, fisioterapisti e logopedisti);
- organismi sanitari pubblici.
Il trattamento può essere effettuato:
- o con il consenso dell'interessato, se il trattamento persegue una finalità di tutela della salute o dell'incolumità fisica del cittadino;
- previa autorizzazione del Garante per la protezione dei dati personali, se il trattamento persegue una finalità di tutela della salute riguardante terzi o la collettività. In questo ultimo caso, quindi, non occorre il consenso dell'interessato;
- oppure in base all'interesse pubblico (ad esempio, i dati possono essere trattati per consentire lo studio di una malattia al fine di curare altre persone).
Il **consenso può essere espresso anche verbalmente**, dall'interessato oppure dal legale rappresentante, da un prossimo congiunto o un familiare o convivente, o dal responsabile della struttura presso cui dimora l'interessato, nel caso di impossibilità fisica o di incapacità di intendere e di volere dell'interessato. Il consenso deve essere preventivo, ma può essere raccolto successivamente se:
- l'interessato è impossibilitato fisicamente, incapace di agire o di intendere e di volere e non è presente una persona abilitata al consenso;
- sussiste un grave rischio per la salute dell'interessato;
- vi sono esigenze di urgenza medica.
In alcuni casi il **consenso può essere semplificato**, ad esempio per gli enti pubblici o privati che erogano diverse prestazioni, che possono rilasciare un'unica informativa e recepire un consenso unico.

Informativa
Prima di procedere alla raccolta dei dati occorre fornire l'informativa al paziente (eventualmente può essere fornita oralmente anche se è preferibile sia scritta). Il documento deve indicare:
- chi è il soggetto che raccoglie i dati;
- le finalità del trattamento;
- le modalità del trattamento;
- la natura obbligatoria o facoltativa del conferimento dei dati e conseguenze per un eventuale rifiuto;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati;
- gli estremi identificativi del titolare;
- le modalità per l'esercizio dei diritti a tutela dei propri dati.

Conservazione
I documenti che contengono dati sanitari devono essere conservati in archivi ad accesso controllato (es. schedari con serratura), e comunque in modo che terzi non possano accedervi.

Diffusione dei dati
I dati sullo stato della salute possono essere forniti anche a terzi, come parenti, familiari, conviventi, conoscenti, personale volontario, purché ovviamente il paziente, se cosciente, sia stato informato e abbia consentito. Occorre comunque rispettare l'eventuale richiesta della persona ricoverata a non rendere note neppure ai terzi legittimati la sua presenza nella struttura sanitaria o le informazioni sulle sue condizioni di salute.

Fascicolo sanitario elettronico
Il **Fascicolo sanitario elettronico** (FSE) è uno strumento informatico che riunisce i dati e i documenti (digitali o digitalizzati) di tipo sanitario e sociosanitario, relativi all'assistito. La sua funzione è di condividere tali dati, e quindi la storia clinica del paziente, tra vari medici o organismi sanitari.
Il fascicolo viene, quindi, aggiornato dalle strutture sanitarie e dai medici. Al FSE possono accedere, oltre al paziente (con modalità sicure, es. smart card), i medici e il personale sanitario autorizzato. Non possono accedere terzi, quali periti assicurativi o datori di lavoro.
Il paziente deve poter scegliere se far costituire o meno un FSE con tutti o alcuni dei dati sanitari che lo riguardano. A tal proposito deve essere informato in merito a chi ha accesso ai suoi dati e come questi possono essere utilizzati. Il consenso alla formazione del FSE deve essere distinto dal consenso alle cure, cioé, ovviamente, il mancato consenso alla costituzione del FSE, oppure semplicemente all'inserimento di alcuni dati nel fascicolo, non può precludere la possibilità di usufruire delle cure.
Il consenso può essere sempre revocato, e il paziente ha il diritto di oscurare alcuni dati specifici dal FSE.

Registro dei Trattamenti

La tenuta del **registro dei trattamenti** è prevista dall'articolo 30 del regolamento generale europeo, ed è considerata indice di una corretta gestione dei trattamenti.
L'onere della tenuta del registro è a carico del titolare e, se nominato, del responsabile del trattamento. La tenuta del registro è utile per una completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzata anche all'analisi del rischio di tali trattamenti e ad una corretta pianificazione dei trattamenti. Per cui le autorità invitano tutti i titolari a dotarsene, eventualmente inserendo negli stessi ogni elemento utile, anche oltre a quelli minimi previsti dalle norme.
Il registro deve essere tenuto in forma scritta, anche in formato elettronico, e va esibito all'autorità di controllo (Garante) in caso di verifiche.

Registro dei titolari del trattamento
Il registro deve elencare una serie di informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, se nominati, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati (DPO);
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie dei dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) 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;
f) dove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) dove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Registro dei responsabili del trattamento
Il paragrafo 2 dell'articolo 30 del GDPR prevede che anche i responsabili del trattamento debbano tenere un registro simile in relazione alle attività svolte per conto del titolare. Il contenuto deve essere il seguente:
- 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 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, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Esenzioni
Sono **esentate dall'obbligo di tenuta del registro le imprese o le organizzazioni con meno di 250 dipendenti**, a meno che il trattamento effettuato:
- possa presentare un rischio per i diritti e le libertà degli interessati,
- non sia occasionale,
- o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 (cioé dati sensibili o giudiziari).
Per il concetto di **rischio** sovviene il Considerando 75 del GDPR:
"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione

economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati".

Parere del Gruppo Articolo 29

Il Working Party Article 29 ha pubblicato un parere sul registro dei trattamenti (qui il link al parere). Nel parere precisa che **è sufficiente che occorra una sola delle condizioni previste dall'articolo 30 per far scattare l'obbligo di tenuta del registro**. Per cui basta trattare dati personali in modo stabile per essere tenuti alla registrazione dei trattamenti.
In tale prospetiva occorre ricordare che qualsiasi azienda tratta dati sensibili (relativi alla salute) dei propri dipendenti (ad esempio, un'aspettativa per motivi di salute). Anche i liberi professionisti trattano dati personali altrui in maniera non occasionale. Ed anche un sito web con un form di contatti.
Tale interpretazione appare in contrasto con quella dell'Autorità di controllo italiana che ha precisato sul suo sito che tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. In tal senso sarebbe sufficiente avere meno di 250 dipendenti e non effettuare trattamenti a rischio, laddove l'interpretazione del WP29 (che è successiva, e il Garante italiano fa parte del WP29) è molto più ristrettiva.
Il parere del WP29 chiarisce che è sufficiente registrare i soli trattamenti che attivano l'obbliglo dit enuta, e invitano le Autorità nazionali a proporre sui propri siti un modello di registro semplificato per le piccole e medie imprese.

Modello

L'autorità di controllo belga ha predisposto un modello non ufficiale del registro, poi tradotto in inglese (link al modello in inglese).

valutazione del rischio

Il nuovo regolamento generale ha un approccio basato sulla **valutazione del rischio** (*risk based*), piuttosto che sulla protezione dell'utente.
Con tale valutazione si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. Quindi, il **rischio** inerente al trattamento è da intendersi come l'impatto negativo sulle libertà e i diritti degli interessati.
Il Considerando 75 ci aiuta con riferimento al **concetto di rischio**: "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati".

Si tratta di uno dei criteri previsti dal regolamento generale per la progettazione dei trattamenti, che appunto prevede l'**obbligo di una analisi del rischio del trattamento**, e quindi della valutazione delle misure tecniche od organizzative che il titolare ritiene di dover adottare per ridurre l'eventuale rischio.
La **valutazione di impatto del trattamento** (**D.P.I.A.**, cioè *Data Protection Impact Assessment*) è un **onere posto direttamente a carico del titolare del trattamento**, col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali, imponendo al titolare l'onere di una valutazione preventiva delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati.
La valutazione del rischio, da realizzare per ogni singolo trattamento, dovrà portare il titolare a decidere in autonomia se sussistono **rischi elevati** inerenti il trattamento, in assenza dei quali potrà procedere oltre. Se invece ritenesse sussistenti detti rischi, dovrà individuare le **misure specifiche richieste per attenuare o eliminare il rischio** (che non sono indicate dal regolamento).
Solo nel caso in cui il titolare non dovesse trovare misure idonee a eliminare o ridurre il rischio, occorrerà consultare l'Autorità di controllo. L'Autorità interviene solo *ex post*, sulle valutazioni del titolare, indicando le misure ulteriori eventualmente da implementare, fino ad eventualmente ammonire il titolare o vietare il trattamento.
In ogni caso il titolare dovrà giustificare le sue valutazione e rendicontarle nel registro dei trattamenti.
Il titolare deve consultarsi col DPO (art. 35) quando svolge la valutazione di impatto, il quale DPO ha il compito di fornire, se richiesto, un parere in merito alla valutazione di impatto e sorvegliarne lo svolgimento. Nel caso in cui il titolare non concordi con le indicazioni del DPO dovrà motivare e documentare il suo dissenso.

Casi nei quali la DPIA è necessaria
L'articolo 35 del regolamento europeo regolamenta la valutazione di impatto, stabilendo la sua necessità quando il trattamento prevede l'uso di nuove tecnologie e può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. In particolare l'articolo 35 evidenzia la necessità della valutazione di impatto nei seguenti casi:

- il trattamento determina 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;
- il trattamento riguarda dati sensibili o giudiziari su larga scala;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Le Autorità di controllo hanno un ruolo importante, in quanto possono stabilire, con un elenco pubblico, quali tipologie di trattamenti richiedono comunque la valutazione di impatto. Allo stesso modo, possono redigere un elenco delle tipologie di trattamenti per i quali la valutazione non è necessaria.

Contenuto minimo

La valutazione di impatto deve contenere almeno:
- la descrizione sistematica dei trattamenti previsti, la finalità del trattamento, compreso l'interesse legittimo perseguito dal titolare;
- la valutazione dei rischi;
- le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento.

PIA tool
Il CNIL (autorità di controllo francese) ha messo a disposizione un software open source per la valutazione di impatto sia nella versione standalone (da scaricare sul computer) che in quella online. Anche il Garante italiano segnala questo software come tool per realizzare la valutazione.

Video

Legittimo interesse

Il **legittimo interesse** del titolare del trattamento può costituire la base giuridica del trattamento dei dati, purché siano bilanciati i diritti tra il titolare e l'interessato.
Con la normativa precedente al GDPR, il **bilanciamento tra i diritti delle parti** era demandato all'Autorità per la protezione dei dati personali, cosa che ha limitato l'utilizzo di questa base giuridica per il trattamento. L'articolo 24, lettera g), del Codice della privacy prevedeva, appunto, la possibilità di trattare dati, con esclusione della diffusione (a differenza della direttiva europea, scelta questa del legislatore proprio per demandare il bilanciamento al solo Garante), nei casi individuati dai Garanti per perseguire un legittimo interesse di un titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato.
Nell'ambito del nuovo **principio di responsabilizzazione**, con il Regolamento generale europeo (GDPR) **compete, invece, alle aziende effettuare tale bilanciamento**, consentendone un'applicazione generalizzata, fermo restando la possibilità di verifica successiva da parte del Garante. L'azienda dovrà, quindi, determinare se le sue azioni sono in linea con le ragionevoli aspettative dell'utente. Si tratta, purtroppo, di termini vaghi che potrebbero consentire abusi nel trattamento dei dati. Il bilanciamento degli interessi contraposti, infatti, è un'operazione complessa. Concedere ai privati la possibilità di tarsi le leggi su misura, ricorrendo ad una valutazione discrezionale dei contrapposti interessi, potrebbe condurre anche alla vanificazione della normativa, sicuramente ad un'incertezza applicativa in grado di alimentare controversie e diseguaglianze.

Requisiti
Se il trattamento è basato sui legittimi interessi non occorre il consenso dell'interessato, **purché, però, non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato** (in special modo se questi è un minore) **tenuto conto delle ragionevoli aspettative dello stesso in base alla relazione col titolare del trattamento** (Considerando 47 del Regolamento Generale europeo).
Occorre però informare l'interessato del fatto che i suoi dati sono trattati in base ai legittimi interessi, senza però che sia necessario spiegare come il titolare opera il bilanciamento tra i diritti.
Per l'utilizzo dei legittimi interessi quale base giuridica del trattamento occorrono alcuni requisiti:
1) il titolare del trattamento ha necessità **di elaborare il dato** per fini propri o di terzi (ad esempio, se una società finanziaria cerca un suo cliente che è in ritardo coi pagamenti, la società ha il legittimo interesse ad ottenere il nuovo indirizzo del cliente anche in assenza di consenso specifico);
2) occorre **bilanciare gli interessi del titolare con quelli dell'interessato**, e quindi il trattamento appare ingiustificato se ha degli effetti pregiudizievoli sui diritti e le libertà, o interessi legittimi, del singolo (riportandoci all'esempio di prima, è evidente che l'interesse del cliente a non pagare le tasse non può essere ritenuto legittimo o giustificato);
3) il trattamento delle informazioni deve essere **equo e rispettare i principi di protezione dei dati (q**uindi la società finanziaria deve garantire che i dati siano precisi, aggiornati, non eccessivi -la società ottiene solo i dati necessari allo scopo, rintracciare il cliente-.
Anche se il Regolamento non contiene un elenco tassativo dei casi di "legittimo interesse", il Considerando 47 si esemplificano alcune circostanze nelle quali possono sussistere **motivi legittimi per il trattamento**, cioè "*quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento*". Ovviamente non si tratta di un'autorizzazione generalizzata al trattamento dei dati, ma è sempre richiesta un'attenta valutazione al fine di verificare se i diritti dell'interessato possano prevalere sui legittimi interessi del titolare, nel caso in cui, ad esempio, l'interessato può ragionevolmente attendersi che non vi sia un ulteriore trattamento dei suoi dati.
In conclusione, l'azienda, prima di iniziare qualsiasi trattamento dei dati sulla base dei legittimi interessi, deve non solo valutare se ha correttamente preso in considerazione tutti i rischi in gioco, ma anche raccogliere (e documentare, vedi registro dei trattamenti) elementi sufficienti per essere in grado di dimostrare che gli interessi relativi sono stati ben bilanciati tra loro. I titolari dovrebbero mantenere un registro delle valutazione in tema di legittimi interessi al fine di provare il corretto bilanciamento dei diritti.

Casi pratici
In base al Considerando 47, Il trattamento dei dati per finalità di marketing diretto può essere considerato legittimo interesse. Il fatto di menzionare espressamente il marketing diretto quale trattamento ammesso in base ai legittimi interessi, però, non autorizza l'azienda ad un trattamento libero dei dati personali, dovendo essa comunque contemperare i suoi interessi con i diritti della persona e con gli stessi interessi particolari degli interessati al trattamento. Ad esempio, **se l'interessato è già cliente** dell'azienda sussiste il bilanciamento dei diritti.

L'interesse legittimo deve essere reale e non troppo vago. Ad esempio, può essere applicato all'elaborazione dei dati in funzione della **protezione contro le frodi**, per **misura di sicurezza**, o il **trasferimento di dati tra parti diverse della stessa azienda**. E questo specialmente nel caso in cui l'interessato si aspetta quel tipo di elaborazione dei dati.
Ulteriori casi nei quali possono essere invocati i legittimi interessi per il trattamento dei dati sono:
- elaborazione al fine di verifica dell'età;
- valutazione del rischio;
- per l'esercizio del diritto di opposizione (vedi paragrafo successivo) ad esempio nel marketing diretto, nel qual caso può essere necessario mantenere la mail per impedire l'invio di ulteriori comunicazione commerciali;
- personalizzazione del sito web per migliorare l'esperienza dell'utente;
- per analisi web, verifica del numero di visitatori del sito, commenti, ecc...;
- per la comunicazione di reati all'autorità giudiziaria;
- in ambito lavorativo l'utilizzo di dati di localizzazione (smartphone, GPS).

Opposizione dell'interessato
Nel caso di trattamenti basati su legittimi interessi, **l'interessato ha il diritto di opporsi**, in qualsiasi momento e gratuitamente, al trattamento dei dati personali che riguardano la sua situazione particolare (Considerando 70 del Regolamento Generale). Incombe sul titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato. L'interessato deve essere informato della possibilità di avvalersi tale diritto (tramite l'informativa).
Ricordiamo che in base ai legittimi interessi non è possibile trattare i dati sensibili, per i quali occorre il consenso.

Provvedimenti del Garante
In relazione ai lgittimi interessi, il Garante Privacy italiano ha emesso vari provvedimenti dai quali si possono desumere alcuni parametri per un corretto bilanciamento:
- provvedimento su misure biometriche (2014);
- provvedimento su videosorveglianza (2010);
- verifica preliminare su transazioni commerciali (2017), col quale è stato ritenuto ammissibile un trattamento aziendale di dati connesso ad un sistema antifrode;
- verifica preliminare su banca dati in ambito assicurativo (2017).

Modifiche a seguito della legge di bilancio 2018
Con la legge di bilancio del 2018 (Legge 27 dicembre 2017, n. 205, G.U. n.302 del 29-12-2017 - Suppl. Ordinario n. 62 - commi da 1020 a 1024-), il legislatore italiano mostra di non gradire molto l'utilizzo dei legittimi interessi quale base giuridica di un trattamento. Infatti, la finanziaria prescrive che i responsabili del trattamento dei dati che trattano i dati personali mediante mezzi automatizzati o " nuove tecnologie " sulla base dei legittimi interessi devono:
- inviare una **notifica preventiva** all'Autorità Garante per la protezione dei dati, allegando una nota informativa (informativa sulla privacy o semplicemente un modello per fornire dettagli sull'attività di trattamento dei dati da non incorporare nell'informativa sulla privacy, non è chiaro!) da redigere secondo un modello e le linee guida che l'autorità emetterà;
- attendere l'approvazione dell'autorità, ma nel frattempo, trascorsi 15 giorni dall'invio del materiale all'autorità, potrà comunque iniziare il trattamento (non è un consenso tacito, in quanto l'autorità comunque proseguirà la sua verifica).
In questo modo di fatto si replica l'approvazione prevista con la precedente normativa modificando le norme previste dal regolamento europeo che dovrebbe, invece, applicarsi senza alcuna modifica a tutti gli Stati dell'Unione europea. Introducendo, inoltre, un controllo preventivo che è in contrasto con il principio di responsabilità alla base del GDPR.
E' ovvio che la norma creerà anche problemi pratici, visto che oggi tutti i trattamenti sono basati su mezzi automatizzati e quindi l'autorità sarà subissata di notifiche.

Se dovesse rimanere tale limitazione, il trattamento di dati a fini di **marketing diretto** potrà essere operato in base all'art. 88, comma 3, dello schema di Decreto attuativo del Regolamento europeo (Decreto in attesa di approvazione).