FISCOPIÙ

Privacy

di **Gianluca Natalucci**

Bussola del 25 maggio 2018

A partire dal 25 maggio 2018 entra in vigore in Italia il Regolamento UE 2016/679 (definito come GDPR) relativo alla protezione dei dati personali, nonché alla loro libera circolazione. Tale disposizione comunitaria sarà direttamente applicabile ed entrerà in vigore abrogando la previgente normativa in tema di privacy contenuta nella Direttiva 95/46/CE. In Italia, il recepimento del Regolamento ha fatto sì che venisse sostituita a tutti gli effetti la disciplina della privacy contenuta all'interno del Codice della Privacy, istituita con il D.Lgs. n. 196/2003. Tale abrogazione, disposta dal Consiglio dei Ministri nell'Atto di Governo 022 (attualmente all'esame in Parlamento), è stata sancita al fine di coordinare e semplificare la disciplina della privacy. L'obiettivo di questa nuova normativa sulla privacy è quello di coordinare le norme vigenti a livello europeo e di uniformare il sistema sanzionatorio penale e amministrativo in materia, partendo da ciò che veniva previsto dal Codice della privacy e dalle disposizioni in materia degli altri Paesi europei.

SOMMARIO: 1. Inquadramento - 2. Ambito soggettivo ed oggettivo - 3. Titolare del trattamento e responsabile - 4. Il responsabile per la protezione dei dati (RPD o DPO) - 5. Consenso al trattamento e diritti dell'interessato - 6. Regole generali per il trattamento dei dati - 7. Registro dei trattamenti - 8. Misure di sicurezza e informativa - 9. Notificazione delle violazioni dei dati personali - 10. Cessazione del trattamento - 11. Tutela dell'interessato e sanzioni - 12. La Privacy negli studi professionali - 13. Riferimenti

1. Inquadramento
L'entrata in vigore del Regolamento 2016/679 (Regolamento GDPR - *General Data Protection Regulation*) ha comportato un notevole cambiamento in materia di *Privacy* e di trattamento dati.

Il Regolamento, infatti, introduce nuove norme finalizzate alla protezione dei diritti e delle libertà fondamentali delle persone fisiche relativamente ai dati personali.

Tale provvedimento, pur essendo direttamente applicabile nei paesi dell'UE senza necessità di recepimento, ha previsto in ogni caso l'intervento da parte del legislatore italiano, il quale è voluto intervenire per cercare di **agevolare il passaggio da quanto veniva disposto precedentemente** dal Codice della *Privacy*, **a quello che viene disposto con il GDPR**, eliminando, da un lato, quelle disposizioni del Codice che non potevano essere più considerate valide alla luce delle nuove disposizioni e dall'altro, mantenendo applicabili quelle che invece vengono ancora riprese dallo stesso Regolamento.

A tal proposito, è attualmente al vaglio del Parlamento uno schema di Decreto Legislativo (AG 22/2018) recante la **nuova disciplina del Codice della *Privacy*** di cui al D.Lgs. n. 196/2003 modificato per recepire il Regolamento GDPR, il quale è stato approvato dal Garante della *Privacy* con il provvedimento del **22 maggio 2018**.

In particolare, il Regolamento delinea le regole per il **trattamento dei dati** al fine di tutelare i soggetti interessati stabilendo l'ambito oggettivo e soggettivo, i diritti dei soggetti interessati, le norme per il trasferimento dei dati, nonché le sanzioni applicabili.
Sono, inoltre, stati previsti alcuni **principi** ai quali devono attenersi gli utilizzatori dei dati personali al fine di non ledere la *Privacy* di coloro da cui vengono reperite le informazioni; l'art. 5 prevede infatti quanto segue:

- i **dati personali** devono essere **trattati in modo lecito, corretto e trasparente nei confronti dell'interessato**;
- **devono essere raccolti per precise finalità** esplicitate e legittimate e trattati in maniera compatibile con le stesse finalità;
- tali **dati devono essere adeguati, pertinenti e limitati, oltre che esatti e aggiornati**;
- **devono essere conservati** in maniera tale **da consentirne l'identificazione degli interessati** per un periodo non superiore a quello previsto per raggiungere le finalità;
- **trattati con adeguata sicurezza**;
- **il titolare del trattamento deve essere in grado di comprovare il rispetto dei predetti principi**.

Principi applicabili al trattamento dei dati personali (art. 5 - Regolamento UE GDPR)	
LICEITÀ, CORRETTEZZA E TRASPARENZA	**LIMITAZIONE DELLA FINALITÀ**
MINIMIZZAZIONE DEI DATI	**ESATTEZZA**
LIMITAZIONE DELLA CONSERVAZIONE	**INTEGRITÀ E RISERVATEZZA**
RESPONSABILIZZAZIONE	

Il **principio di responsabilizzazione è il punto cardine della riforma della normativa *Privacy***, considerando il passaggio da un sistema autorizzatorio ad uno basato sull'***accountability*** (responsabilità) dei titolari e dei responsabili.
Tali soggetti, infatti, dovranno essere in grado di dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento. A tal proposito l'art. 25 del Regolamento prevede l'applicazione del criterio "*data protection by default and by design*", ossia la necessità di progettare il trattamento prevedendo fin dall'inizio:

- le **garanzie indispensabili** al fine di rispettare il Regolamento stesso e i diritti degli interessati;
- i **possibili rischi** legati al trattamento.

L'intervento delle autorità di controllo sarà principalmente "*ex post*", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare.

2. Ambito soggettivo ed oggettivo
Come si accennava, il GDPR dispone la protezione della tutela dei diritti e delle libertà fondamentali nei confronti delle **persone fisiche**, così come previsto dall'art. 1, in materia di dati personali e della loro circolazione, **affermando l'esclusione dalla suddetta disciplina nei confronti delle persone giuridiche,** ovvero imprese e enti.

In evidenza: Definizione di dati personali (art. 4, Reg. GDPR)

Per **dati personali** si intendono tutte quelle informazioni riferite direttamente o indirettamente ad una persona fisica (soggetto interessato) e che le permettono di poter essere identificata o resa identificabile.
Sono da considerare rientranti nella categoria i dati personali:

- i **dati anagrafici (nome e cognome)**;
- il **numero di conto corrente**;
- lo **stato di salute**;
- le **informazioni riferibili alla fisicità di un soggetto**, come foto e video.

Sono, inoltre, compresi nella nuova disciplina i **dati pseudonimizzati**, ossia quei dati personali che non possono essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Non rientrano nella disciplina del Regolamento i dati anonimi, cioè le informazioni che riguardano una persona fisica che non è possibile identificare.

La disciplina regola il trattamento dei dati personali, dove per trattamento si intende 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.

In merito al trattamento dei dati personali, l'art. 9 del Regolamento GDPR fa alcune specifiche.
Il paragrafo 1, infatti, **pone il divieto di trattare dati personali** che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (**cd. dati sensibili**).
Tuttavia, è possibile **derogare** al precedente divieto quando:

- 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 dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
- il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento è effettuato da enti che perseguono finalità politiche, religiose, ecc. nell'ambito della loro attività e con riguardo unicamente a:
    - membri;
    - *ex* membri;
    - altre persone in contatto con l'ente stesso;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
- il trattamento è necessario per finalità mediche; in tal caso è necessario che i dati siano trattati sotto la responsabilità di un professionista soggetto al segreto professionale;
- 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;
- il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'art. 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Il Regolamento trova la sua applicazione **per i soggetti a cui si applica il diritto dell'Unione Europea**.
A tal proposito, l'art. 3 del citato Regolamento prevede che lo stesso deve essere rispettato:

- dai **titolari del trattamento o** dal **responsabile qualora** il relativo **stabilimento sia situato**

nell'Unione Europea, anche se poi il trattamento è effettuato in territori *extra* UE;
- dal **titolare o dal responsabile non stabilito in UE**, **quando** le attività di trattamento riguardano:
    - soggetti interessati che si trovano nell'UE;
    - l'offerta di beni o la prestazione di servizi nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
    - il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

L'art. 2 individua anche delle **ipotesi di esclusione dall'ambito di applicazione del nuovo Regolamento**. Infatti, **non è riconosciuto come doveroso**, ai sensi dell'art. 2, il rispetto di tale disciplina quando "*il trattamento dei dati è effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o di sanzioni penali*", o nel caso in cui il trattamento dei dati venga effettuato da una persona fisica all'interno nel nucleo personale o domestico.

Inoltre, il **Regolamento GDPR non si applica** quando i trattamenti dei dati personali:

- sono **raccolti per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione**;
- sono **effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE**;
- sono **richiesti da una persona fisica per l'esercizio di attività a carattere esclusivamente personale domestico**.

Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il Regolamento (CE) n. 45/2001.
Il Regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'art. 98.

3. Titolare del trattamento e responsabile
La seguente tabella fornisce una sintesi dei soggetti che possono intervenire nel trattamento dei dati.

TITOLARE DEL TRATTAMENTO	È l'entità nel suo complesso, o l'unità od organismo periferico, che esercita un potere decisionale del tutto autonomo sulle **finalità** e sulle **modalità del trattamento**, ivi compreso il profilo della sicurezza (una persona giuridica, una pubblica amministrazione o un qualsiasi altro ente, associazione od organismo). Si tratta di una figura che è stata nuovamente ripresa nel GDPR, all'interno del quale sono stati definiti in maniera più precisa i relativi compiti. Il **titolare del trattamento** è colui il quale, nel momento in cui effettua il trattamento presso l'interessato, è soggetto, ai sensi degli artt. 13 e 14, ad **obbligo di informativa**, in quanto deve fornire

informazioni in merito a:

- identità e dati di contatto;
- dati di contatto del responsabile della protezione dei dati;
- finalità del trattamento;
- eventuali destinatari;
- eventuale intenzione al trasferimento dei dati personali verso un Paese terzo.

Inoltre, per consentire un **trattamento più chiaro**, il Regolamento prevede **ulteriori informazioni da fornire**, tra cui:

- il periodo di conservazione dei dati personali;
- il diritto dell'interessato nel richiedere l'accesso, la rettifica o la cancellazione dei dati personali;
- la revoca al consenso;
- il diritto a proporre richiamo all'autorità di controllo;
- l'esistenza di un processo decisionale automatizzato;
- conclusione del contratto.

La **Guida Garante Privacy 2018** dispone in merito che: "*è opportuno che i titolari di trattamento verifichino la rispondenza delle informative attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del Regolamento*".
L'art. 26 del suddetto Regolamento prevede anche la presenza di **più di un titolare**, definito come **contitolare**.
I contitolari devono determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

	Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato. Indipendentemente da ciò, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento.
RESPONSABILE DEL TRATTAMENTO	Si tratta di una figura ripresa all'interno del Regolamento, il quale viene designato **facoltativamente** dal titolare tra soggetti che per **esperienza, capacità ed affidabilità** assiste il titolare del trattamento **con misure tecniche e organizzative** adeguate e **garantisce il rispetto degli obblighi** disposti dagli artt. 32-36. Tale soggetto viene designato attraverso un **contratto**, il quale deve rispettare le disposizioni di cui all'art. 28, par. 3. Sia i titolari sia i responsabili (compreso il responsabile per la protezione dei dati), in virtù del principio di responsabilizzazione sancito dall'art. 25, sono tenuti ad adottare comportamenti idonei a dimostrare il rispetto del Regolamento.
RESPONSABILE PER LA PROTEZIONE DEI DATI (RPD o DPO)	Il **responsabile per la protezione dei dati è una nuova figura** introdotta dal GDPR (art. 37, Regolamento GDPR). Si tratta di un soggetto che viene nominato in specifici casi, ad esempio quando: • il trattamento dei dati viene svolto da un'autorità pubblica; • le attività del titolare sono finalizzate al monitoraggio degli interessati su larga scala; • le attività del titolare sono finalizzate al trattamento di dati particolari e viene svolto su larga scala dei dati sensibili di cui agli artt. 9 e 10 del Regolamento. Nei confronti della **Pubblica Amministrazione la presenza di tale soggetto è ritenuta sempre obbligatoria.** Tale ruolo può essere ricoperta da: • un dipendente del titolare; • un responsabile; • un soggetto esterno. Si tratta di un soggetto professionale per la quale non sono ancora stati stabiliti i requisiti per poter ricoprire tale carica, anche se tuttavia si ritiene che debba trattarsi di un soggetto con

	professionalità e **competenza**. Il DPO si occupa di intervenire assieme ai soggetti sopra citati affinché il **trattamento dei dati** venga realizzato **conformemente** rispetto a quanto previsto dal **Regolamento**. Oltre a tale ruolo, il DPO possiede **altri compiti** definiti dall'art. 39, i quali dovranno **esplicitamente** essere **descritti all'interno del contratto**. "*I DPO **non rispondono personalmente** in caso di **inosservanza del RGPD**. Spetta al titolare del trattamento o al responsabile del trattamento garantire di essere in grado di **dimostrare che le operazioni di trattamento sono conformi con le disposizioni del Regolamento stesso***" (Linee Guida del gruppo di lavoro "Articolo 29"). Anche perché nei confronti di tali soggetti può essere richiesta la prova della messa in conformità del Regolamento da parte dell'Autorità Garante.

Il Garante per la protezione dei dati personali

Il Garante è **organo collegiale** costituito da **quattro componenti**, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato, che **opera in piena autonomia** e con **indipendenza di giudizio e di valutazione**.

I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

I componenti eleggono nel loro ambito un **presidente**, il cui voto prevale in caso di parità e un **vicepresidente** che assume le funzioni del presidente in caso di sua assenza o impedimento.

Il **presidente e i componenti durano in carica quattro anni e non possono essere confermati per più di una volta**; per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.

Alle dipendenze del Garante è posto l'**Ufficio del Garante**.
Anche con il Regolamento, la figura del **Garante** assume un ruolo fondamentale in qualità di **autorità di controllo che ogni Stato membro deve disporre**, in merito alla valutazione della conformità dei trattamenti dei dati personali rispetto al Regolamento.

In evidenza: compiti del Garante (come disciplinato dal Regolamento GDPR)
Ogni autorità di controllo possiede **poteri** relativi a:

- richiesta, nei confronti del titolare e dei responsabili al trattamento, di fornire le informazioni relativi all'esecuzione dei compiti;
- revisione della protezione dei dati;
- correttivi, tra questi:
  - avvertimento o ammonimento nei confronti dei titolari o dei responsabili per violazione del Regolamento;
  - richiedere l'eliminazione delle violazioni, fino alla cancellazione dei dati oggetto della verifica;
  - erogare sanzioni;
- autorizzativi/consultativi, tra questi:
  - rilascio di pareri e consulenze;
  - autorizzazione ai trattamenti;
  - adozione delle clausole di protezione.

Il Regolamento riconferma, quindi, i compiti riconosciuti verso tale autorità di controllo, prevedendo, inoltre, la **possibilità di emettere sanzioni fino al 4% del fatturato mondiale**.

4. Il responsabile per la protezione dei dati (RPD o DPO)

Come si accennava, il **RPD** è una nuova figura introdotta dal Regolamento GDPR ed è regolamentata principalmente dagli artt. 37-39 dello stesso Regolamento.

Oltre a quanto precedentemente detto, si riportano qui di seguito i compiti del responsabile per la protezione dati:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa;
- vigilare sull'osservanza delle norme e delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati;
- cooperare con l'autorità di controllo.

A tal fine, il titolare del trattamento e il responsabile del trattamento devono coinvolgere tempestivamente e adeguatamente il RPD in tutte le questioni riguardanti la protezione dei dati personali.

In data **18 maggio 2018**, il Garante per la protezione dei dati personali ha attivato la **procedura per la comunicazione del nominativo del responsabile per la protezione dei dati** prescelto esperibile direttamente dal sito istituzionale al seguente *link https://servizi.gpdp.it/comunicazione-rpd/*.

5. Consenso al trattamento e diritti dell'interessato

Il trattamento di dati personali da parte di persone fisiche, di **età superiore ai 16 anni** (prima di tale età il consenso deve essere raccolto dei genitori, o di chi ne fa le veci), è ammesso solo con il **consenso espresso** (in forma scritta quando il trattamento riguarda dati sensibili) dell'interessato, che può riguardare l'intero trattamento o una o più operazioni.

In ogni caso, **il consenso è validamente prestato** solo se:

- è espresso liberamente e in riferimento ad un trattamento chiaramente individuato;
- è documentato per iscritto;
- le informazioni necessarie sono state rese all'interessato;
- deve essere manifestato attraverso la dichiarazione positiva inequivocabile;
- le categorie dei dati personali;
- le finalità del trattamento;
- i destinatari a cui i dati personali sono stati o saranno comunicati;
- il periodo di conservazione dei dati, o quando non è possibile, i criteri utilizzati per determinare tale periodo;
- la rettifica, la cancellazione, o la limitazione del trattamento dei dati personali;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- la possibilità di proporre reclamo ad un'autorità di controllo;
- qualora i dati siano trasferiti a un Paese terzo, l'interessato ha diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'art. 46.

Rispetto a quanto veniva previsto precedentemente dal Codice della *Privacy*, il **diritto di accesso**, disposto dall'art. 15, prevede che l'interessato ha sempre il diritto di ricevere una **copia** dei dati personali oggetto del trattamento.

In merito al **diritto di rettifica**, il Regolamento prevede, all'art. 16, che l'interessato abbia **diritto di ottenere la rettifica dei propri dati inesatti, o l'integrazione di dati personali incompleti**.

L'interessato ha inoltre **diritto di opporsi**, in qualsiasi momento:

- per **motivi legittimi** legati al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- al trattamento di dati personali che lo riguardano a fini del ***marketing* diretto**.

I diritti appena descritti sono **esercitati con richiesta** rivolta senza formalità al titolare o al responsabile (anche tramite un incaricato), della quale deve essere fornito apposito riscontro **entro un mese**, anche in caso negativo, **estendibile fino a 3 mesi** in casi di particolare complessità.

Occorre precisare che il GDPR interviene riconoscendo nei confronti del soggetto interessato altri diritti, come:

- il diritto all'**oblio**;
- il diritto di **limitazione al trattamento dei dati personali**;
- il diritto alla **portabilità dei propri dati**.

In primis, il **diritto all'oblio permette la cancellazione dei dati personali** da parte del titolare del trattamento, quando questo viene richiesto dall'interessato.

Tale diritto, tuttavia, trova la sua applicazione in presenza di una delle due condizioni disposte dall'art. 17 del Regolamento stesso, ovvero:

- in caso di trattamento dei dati illecito;
- nel caso di esercizio del diritto di opposizione, o di revoca del consenso;
- nell'ipotesi in cui i dati non sono più necessari rispetto alle finalità per le quali erano stati raccolti;
- nel caso in cui quando il trattamento dei dati era stato autorizzato in riferimento ad un soggetto interessato ancora minorenne.

Vengono previste **circostanze di limitazione** all'esercizio di tale diritto nei casi di:

- tutela del diritto alla libertà di espressione o di informazione;
- perseguimento di un interesse pubblico;
- richiesta esplicita dalla legge.

In merito al **diritto alla limitazione**, esso consiste nella **possibilità di richiedere** da parte del soggetto interessato **la sospensione per un certo lasso temporale** di ogni trattamento dei dati. Tale limitazione viene prevista solo in determinate circostanze, come:

- verifica dell'esattezza dei dati;
- trattamento illecito dei dati personali;
- esercizio di un diritto in sede giudiziaria;
- bilanciamento tra interessi del titolare del trattamento e dell'interessato.

Infine, il **diritto alla portabilità** dei dati di cui all'art. 20 del Regolamento GPDR prevede la possibilità per il soggetto interessato di ricevere i dati personali che sono stati trattati e di trasferirli ad un altro titolare del trattamento.

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare (si veda il considerando 68 per maggiori dettagli).
Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile (a tal fine si vedano le Linee Guida sul diritto alla portabilità dei dati emanate dal gruppo di lavoro "Articolo 29" per la protezione dei dati).

Modalità di esercizio
Al momento non sono ancora definite le modalità con le quali è possibile esercitare i propri diritti, ma si ritiene che sia compito del titolare quello di renderle note al momento della trattazione. Precedentemente, la richiesta al titolare (o al responsabile) può essere trasmessa mediante:

- lettera **raccomandata**;
- ***telefax***;
- **posta elettronica**.

L'interessato può inoltre conferire **delega** o procura (per iscritto) a persone fisiche, enti, associazioni od organismi, e può farsi assistere da una persona di fiducia.

In evidenza: dati personali concernenti persone decedute
I diritti riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

L'**identità dell'interessato** viene verificata in base ad **atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento**, mentre la persona che eventualmente agisce per conto dell'interessato deve inoltre esibire o allegare copia dell'apposita **procura**.

Riscontro all'interessato

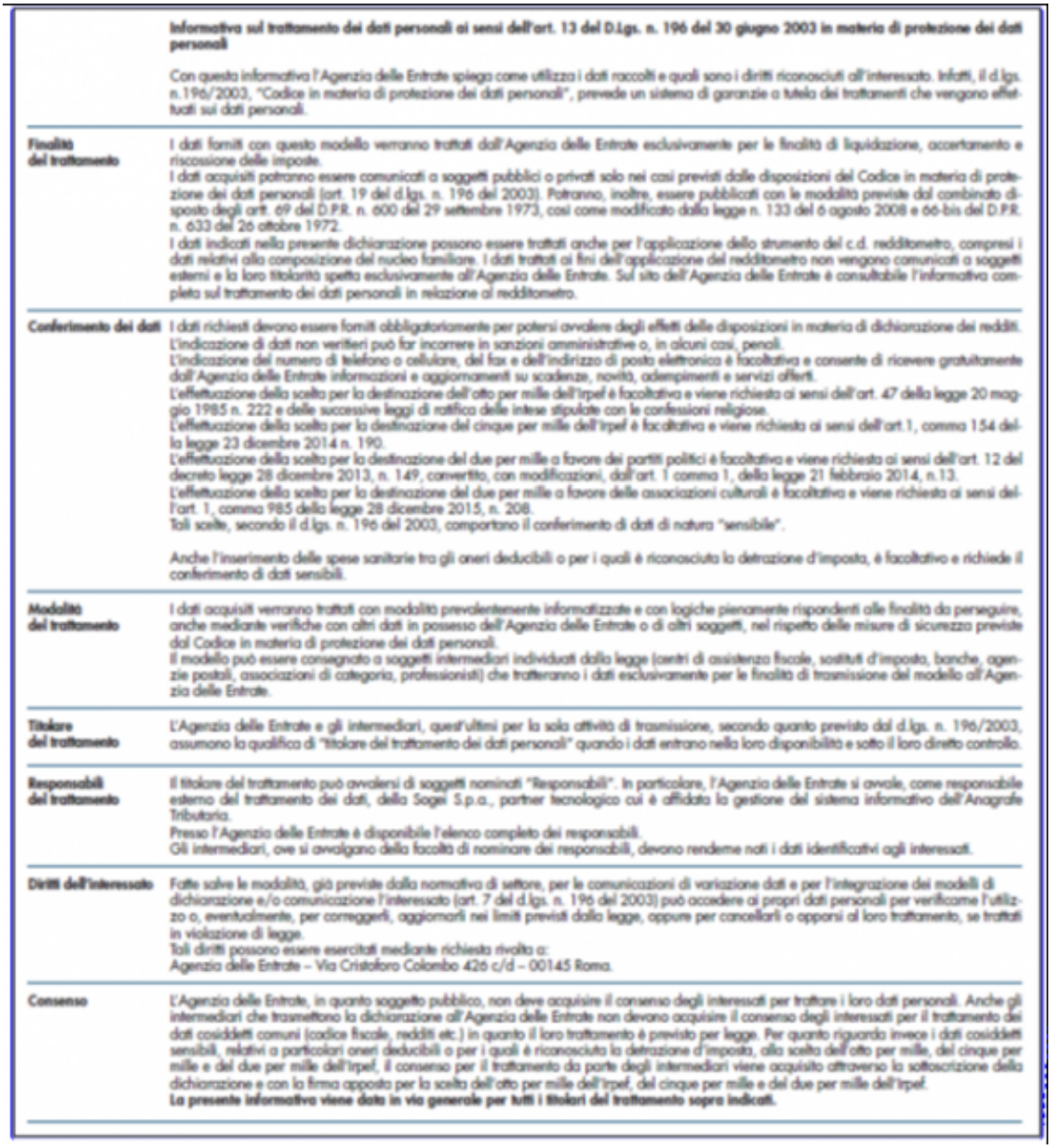
La **risposta** fornita all'interessato non deve essere solo "**intellegibile**", ma anche **coincisa**, **trasparente e facilmente accessibile**, oltre ad utilizzare un **linguaggio semplice e chiaro**, in virtù dell'applicazione del **principio di trasparenza,** sancito dall'art. 12 del Regolamento (Guida Garante *Privacy* 2018).

Al fine di garantire l'effettivo esercizio dei diritti il titolare del trattamento è tenuto ad applicare **misure** volte ad **agevolare l'accesso ai dati** da parte dell'interessato (ad esempio attraverso appositi programmi), a semplificare le modalità di fruizione e a ridurre i tempi per il riscontro al richiedente.

Il **riscontro** deve essere redatto **in forma scritta**, anche attraverso strumenti elettronici che ne favoriscono l'accessibilità; viene, tuttavia, ammessa una **deroga alla forma scritta** nel solo caso in cui venisse **espressamente richiesto** dall'interessato.

In evidenza: riscontro di tutti i dati comunque tratti
Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare.

In evidenza: contributo
Spetta al titolare valutare la complessità del riscontro all'interessato e **stabilire l'ammontare dell'eventuale contributo** da chiedere all'interessato nel solo caso di richieste infondante o eccessive.



Informativa sul trattamento dei dati personali ai sensi dell'art. 13 del D.Lgs. n. 196 del 30 giugno 2003 in materia di protezione dei dati personali

Con questa informativa l'Agenzia delle Entrate spiega come utilizza i dati raccolti e quali sono i diritti riconosciuti all'interessato. Infatti, il d.lgs. n.196/2003, "Codice in materia di protezione dei dati personali", prevede un sistema di garanzie a tutela dei trattamenti che vengono effettuati sui dati personali.

Finalità del trattamento

I dati forniti con questo modello verranno trattati dall'Agenzia delle Entrate esclusivamente per le finalità di liquidazione, accertamento e riscossione delle imposte.
I dati acquisiti potranno essere comunicati a soggetti pubblici o privati solo nei casi previsti dalle disposizioni del Codice in materia di protezione dei dati personali (art. 19 del d.lgs. n. 196 del 2003). Potranno, inoltre, essere pubblicati con le modalità previste dal combinato disposto degli artt. 69 del D.P.R. n. 600 del 29 settembre 1973, così come modificato dalla legge n. 133 del 6 agosto 2008 e 66-bis del D.P.R. n. 633 del 26 ottobre 1972.
I dati indicati nella presente dichiarazione possono essere trattati anche per l'applicazione dello strumento del c.d. redditometro, compresi i dati relativi alla composizione del nucleo familiare. I dati trattati ai fini dell'applicazione del redditometro non vengono comunicati a soggetti esterni e la loro titolarità spetta esclusivamente all'Agenzia delle Entrate. Sul sito dell'Agenzia delle Entrate è consultabile l'informativa completa sul trattamento dei dati personali in relazione al redditometro.

Conferimento dei dati

I dati richiesti devono essere forniti obbligatoriamente per potersi avvalere degli effetti delle disposizioni in materia di dichiarazione dei redditi. L'indicazione di dati non veritieri può far incorrere in sanzioni amministrative o, in alcuni casi, penali.
L'indicazione del numero di telefono o cellulare, del fax e dell'indirizzo di posta elettronica è facoltativa e consente di ricevere gratuitamente dall'Agenzia delle Entrate informazioni e aggiornamenti su scadenze, novità, adempimenti e servizi offerti.
L'effettuazione della scelta per la destinazione dell'otto per mille dell'Irpef è facoltativa e viene richiesta ai sensi dell'art. 47 della legge 20 maggio 1985 n. 222 e delle successive leggi di ratifica delle intese stipulate con le confessioni religiose.
L'effettuazione della scelta per la destinazione del cinque per mille dell'Irpef è facoltativa e viene richiesta ai sensi dell'art.1, comma 154 della legge 23 dicembre 2014 n. 190.
L'effettuazione della scelta per la destinazione del due per mille a favore dei partiti politici è facoltativa e viene richiesta ai sensi dell'art. 12 del decreto legge 28 dicembre 2013, n. 149, convertito, con modificazioni, dall'art. 1 comma 1, della legge 21 febbraio 2014, n.13.
L'effettuazione della scelta per la destinazione del due per mille a favore delle associazioni culturali è facoltativa e viene richiesta ai sensi dell'art. 1, comma 985 della legge 28 dicembre 2015, n. 208.
Tali scelte, secondo il d.lgs. n. 196 del 2003, comportano il conferimento di dati di natura "sensibile".

Anche l'inserimento delle spese sanitarie tra gli oneri deducibili o per i quali è riconosciuta la detrazione d'imposta, è facoltativo e richiede il conferimento di dati sensibili.

Modalità del trattamento

I dati acquisiti verranno trattati con modalità prevalentemente informatizzate e con logiche pienamente rispondenti alle finalità da perseguire, anche mediante verifiche con altri dati in possesso dell'Agenzia delle Entrate o di altri soggetti, nel rispetto delle misure di sicurezza previste dal Codice in materia di protezione dei dati personali.
Il modello può essere consegnato a soggetti intermediari individuati dalla legge (centri di assistenza fiscale, sostituti d'imposta, banche, agenzie postali, associazioni di categoria, professionisti) che tratteranno i dati esclusivamente per le finalità di trasmissione del modello all'Agenzia delle Entrate.

Titolare del trattamento

L'Agenzia delle Entrate e gli intermediari, quest'ultimi per la sola attività di trasmissione, secondo quanto previsto dal d.lgs. n. 196/2003, assumono la qualifica di "titolare del trattamento dei dati personali" quando i dati entrano nella loro disponibilità e sotto il loro diretto controllo.

Responsabili del trattamento

Il titolare del trattamento può avvalersi di soggetti nominati "Responsabili". In particolare, l'Agenzia delle Entrate si avvale, come responsabile esterno del trattamento dei dati, della Sogei S.p.a., partner tecnologico cui è affidata la gestione del sistema informativo dell'Anagrafe Tributaria.
Presso l'Agenzia delle Entrate è disponibile l'elenco completo dei responsabili.
Gli intermediari, ove si avvalgano della facoltà di nominare dei responsabili, devono rendeme noti i dati identificativi agli interessati.

Diritti dell'interessato

Fatte salve le modalità, già previste dalla normativa di settore, per le comunicazioni di variazione dati e per l'integrazione dei modelli di dichiarazione e/o comunicazione l'interessato (art. 7 del d.lgs. n. 196 del 2003) può accedere ai propri dati personali per verificarne l'utilizzo o, eventualmente, per correggerli, aggiornarli nei limiti previsti dalla legge, oppure per cancellarli o opporsi al loro trattamento, se trattati in violazione di legge.
Tali diritti possono essere esercitati mediante richiesta rivolta a:
Agenzia delle Entrate – Via Cristoforo Colombo 426 c/d – 00145 Roma.

Consenso

L'Agenzia delle Entrate, in quanto soggetto pubblico, non deve acquisire il consenso degli interessati per trattare i loro dati personali. Anche gli intermediari che trasmettono la dichiarazione all'Agenzia delle Entrate non devono acquisire il consenso degli interessati per il trattamento dei dati cosiddetti comuni (codice fiscale, redditi etc.) in quanto il loro trattamento è previsto per legge. Per quanto riguarda invece i dati cosiddetti sensibili, relativi a particolari oneri deducibili o per i quali è riconosciuta la detrazione d'imposta, alla scelta dell'otto per mille, del cinque per mille e del due per mille dell'Irpef, il consenso per il trattamento da parte degli intermediari viene acquisito attraverso la sottoscrizione della dichiarazione e con la firma apposta per la scelta dell'otto per mille dell'Irpef, del cinque per mille e del due per mille dell'Irpef.
La presente informativa viene data in via generale per tutti i titolari del trattamento sopra indicati.

6. Regole generali per il trattamento dei dati

La seguente tabella riassume le **regole valide per tutti i trattamenti**.

In tale contesto si precisa che i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

REQUISITI DEI DATI PERSONALI OGGETTO DI TRATTAMENTO	trattati in modo lecito, e secondo correttezza e trasparenza.
	raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi.
	esatti e, se necessario, aggiornati.
	adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati.
	conservati in maniera limitata nel tempo, in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. Inoltre, dovrebbero essere cancellati una volta perseguite le finalità di trattamento.
	disporre di misure di sicurezza tali da garantire l'integrità e la sicurezza delle informazioni.

Il GDPR permette **l'utilizzo** dei dati personali per **finalità diverse da quelle iniziali**, soltanto nel caso in cui le **due finalità, iniziale e finale, siano compatibili**. Per valutare la compatibilità occorrerà osservare:

- il nesso;
- il contesto in cui i dati sono stati raccolti;
- la natura dei dati;
- le conseguenze;
- la presenza di garanzie.

Trasferimento dei dati personali

In merito al **trasferimento dei dati personali** il GDPR non ne fornisce una precisa definizione.
Esso può essere inteso come uno **spostamento dei dati personali** dal titolare o dal responsabile al di fuori del territorio europeo, facendo riferimento a quei trasferimenti avvenuti sia in forma diretta, sia a quelli successivi, ovvero quei trasferimenti che si realizzano quando il soggetto a cui sono stati trasferiti i dati li trasferisce a sua volta ad altri.

Quando si vuole effettuare un **trasferimento dei dati all'estero**, il Regolamento prevede che il titolare del trattamento, o il responsabile, adotti uno degli **strumenti previsti dalla disciplina**, i quali erano già contemplati nel Codice della *Privacy*.

Tra questi vengono individuati:

- i trasferimenti che si realizzano verso Paesi che hanno ottenuto una decisione di adeguatezza da parte della Commissione Europea;
- in presenza di garanzie adeguate;
- nel caso in cui il mittente soddisfi una delle deroghe speciali previste dal Regolamento.

Oltre a questi strumenti, ne sono stati introdotti di altri, attribuendone un ordine gerarchico.
È fondamentale che gli interessati vengano informati in merito, al momento della raccolta dei dati e che venga documentato nel proprio **registro di attività** il trattamento di dati per cui è previsto un **trasferimento e le relative garanzie**.

7. Registro dei trattamenti
Tutti i titolari e i responsabili di trattamento di dati personali, fatta eccezione per gli organismi con meno di 250 dipendenti, sono soggetti ad **obbligo di tenuta del "registro dei trattamenti"**, ovvero del registro all'interno del quale sono iscritte le operazioni di trattamento, i cui contenuti sono previsti dall'art. 30.

Sono tenuti, tuttavia, alla tenuta di tale registro anche gli organismi con **meno di 250 dipendenti**, qualora il trattamento:

- presenti un rischio per i diritti e le libertà dell'interessato;
- non sia occasionale;
- includa particolari categorie di dati.

Si tratta di uno strumento obbligatorio inserito con il Regolamento e finalizzato, non solo a permetterne la **supervisione** al **Garante**, ma anche per poter far sì che si disponga di un **quadro aggiornato dei trattamenti interni all'azienda o di un soggetto pubblico**.

Tale **registro** deve essere tenuto in **forma scritta, anche elettronica** e deve essere subito **esibito** qualora venga richiesto dal Garante (Guida Garante *Privacy* 2018).

All'interno dello stesso registro vengono individuati:

- il nome e i dati del titolare del trattamento, del contitolare, del rappresentante del trattamento e del responsabile della protezione dei dati;
- le categorie di interessati e di dati;
- le finalità di trattamento;
- la valutazione dei tipi di dati;
- dove vengono trattati i dati;
- per quanto tempo vengono trattati i dati;
- le misure di sicurezza;
- eventuali trasferimenti verso Paesi terzi.

Registri delle attività di trattamento	
A cura del titolare del trattamento	**A cura del responsabile del trattamento**
Nome e dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati.	nome e 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 finalità del trattamento.	le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento.
descrizione delle categorie di interessati e delle categorie di dati personali.	se 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'art. 49 del Regolamento GDPR, la documentazione delle garanzie adeguate.
le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali.	se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.
se 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'art. 49 del Regolamento GDPR, la documentazione delle garanzie adeguate.	
se possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati.	
se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.	

8. Misure di sicurezza e informativa

Con il GDPR sono intervenuti importanti **cambiamenti** in merito al **sistema di sicurezza** relativo al trattamento dei dati personali.

Rispetto, infatti, a quanto veniva previsto nel Codice della *Privacy* non ci si sofferma più su una serie di strumenti di salvaguardia, ma si cerca di **inquadrare la misura di sicurezza** tale da "*garantire un livello di sicurezza adeguato al rischio*" (art. 32), in maniera tale da:

- evitare di incorrere in casi di violazione di dati;
- eliminare il rischio quando è considerato rilevante;
- tutelare i dati quando questi vengono trasmessi a terzi;

- dimostrare che l'azienda in questione sia a norma.

Le **misure** che il legislatore ha ritenuto rilevanti sono quelle di:

- **natura tecnica**, come ad esempio strumenti di protezione informatica;
- **natura organizzativa**, come ad esempio le regole comportamentali che devono essere assunte dai dipendenti, i ruoli e le funzioni assegnati al personale.

La lista delle misure di sicurezza contenute all'art. 32 **non è esaustiva.** Infatti, la valutazione sull'**adeguatezza** delle **misure di sicurezza** deve essere valutata **caso per caso** al titolare del trattamento, o al responsabile in relazione a quelli che sono **i rischi** individuati. Come rilevato dalla Guida del Garante della *Privacy*, **dal 25 maggio 2018** non potranno esistere obblighi generalizzati di adozione di misure "minime" di sicurezza, in quanto la valutazione sarà *case by case*.

Rispetto a quanto veniva previsto nel Codice della *Privacy*, i **contenuti dell'informativa** sono stati **ampliati**, prevedendo all'art. 13 che, in caso di raccolta dei dati presso l'interessato, il titolare del trattamento è tenuto a trasmette le seguenti informazioni:

- identità e dati di contatto del titolare del trattamento e del suo rappresentante;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento e la base giuridica;
- qualora il trattamento si basi sull'art. 6, par. 1 lett. f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- gli eventuali destinatari dei dati personali;
- l'intenzione del titolare del trattamento di trasferire dati personali a un Paese terzo o a un'organizzazione;
- il periodo di conservazione dei dati;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione degli stessi, o la limitazione al trattamento;
- il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica.

In evidenza: dati personali non raccolti presso l'interessato
Ai sensi dell'art. 14 del Regolamento "*qualora i dati non siano stati ottenuti presso l'interessato, il titolare*

del trattamento fornisce all'interessato le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali in questione;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
*f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'*artt. 46 *o* 47*, o all'*art. 49*, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.*

Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
*b) qualora il trattamento si basi sull'*art. 6*, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;*
c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
*d) qualora il trattamento sia basato sull'*art. 6*, paragrafo 1, lettera a), oppure sull'*art. 9*, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;*
e) il diritto di proporre reclamo a un'autorità di controllo;
f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
g) *l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'*art. 22*, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato"*.

9. Notificazione delle violazioni dei dati personali
A decorrere **dal 25 maggio 2018**, i titolari di trattamenti sono tenuti a notificare al Garante le **violazioni di dati personali** di cui vengono a conoscenza, **entro 72 ore e senza ingiustificato ritardo** (art. 33, Regolamento GPDR).

Tale notificazione avviene soltanto qualora i titolari ritengano che da queste violazioni derivino dei **rischi per i diritti e le libertà degli interessati**.

In merito a tali rischi, il Regolamento dispone una "**valutazione dell'impatto dei trattamenti**".
Il Regolamento **non ha imposto un obbligo**, infatti, possono sussistere casi in cui tale **notificazione non debba essere effettuata**, come quelli disposti dall'art. 34, par. 3:

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

- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Se le **misure** adottate dovessero essere **idonee a mitigare il rischio**, il trattamento dei dati può compiersi; altrimenti, sarà necessario **richiedere l'intervento** dell'autorità di controllo per decidere in che modo far fronte al rischio.

Contenuto notifica (art. 33, Regolamento GPDR)
• descrizione della natura della violazione e, se possibile, le categorie e il numero dei soggetti interessati, nonché delle registrazioni; • nome e contatti del responsabile della protezione dei dati o di un altro soggetto da cui reperire i dati; • le probabili conseguenze; • descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

10. Cessazione del trattamento
In caso di **cessazione** (per qualsiasi causa) di un trattamento i dati sono:

- distrutti;
- ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti (altrimenti la cessione è priva di effetti);
- conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
- conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alle varie disposizioni vigenti.

11. Tutela dell'interessato e sanzioni
In linea generale, l'interessato può rivolgersi al Garante in **tre differenti maniere**:

- mediante **reclamo**, per presentare una violazione della disciplina rilevante in materia di trattamento di dati personali;
- mediante **segnalazione**, se non è possibile presentare un reclamo, al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima;
- mediante **ricorso**, se intende far valere gli specifici diritti di cui all'art. 7 del Codice della *Privacy* (sopra citati).

Si fa presente che il Codice della *Privacy* sarà oggetto di **modifica** da parte dell'attuale Atto di Governo 22, al fine di rendere **compatibile la normativa italiana** con il Regolamento GDPR; pertanto, le misure a tutela

dell'interessato, ricordandosi dei diritti esposti nei paragrafi precedenti, potrebbero cambiare.

Proposizione dei reclami
Il reclamo contiene un'indicazione dettagliata dei **fatti** e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli **estremi identificativi** del titolare, del responsabile, ove conosciuto, e dell'istante, oltre ad un **recapito** per l'invio di comunicazioni.

Esso deve essere inoltre sottoscritto dagli interessati e presentato al Garante senza particolari formalità, con in allegato la **documentazione** utile ai fini della sua valutazione e l'eventuale procura.
Occorre precisare che con il Regolamento **non trova più applicazione la verifica preliminare** compiuta dal Garante.

Ricorsi
Quando l'interessato ritiene che il trattamento violi il GDPR ha diritto di proporre **reclamo a un'autorità di controllo** (**Garante**). Quest'ultimo è tenuto a dare informazioni all'interessato in merito allo stato dell'esito dell stesso reclamo.

Tuttavia, secondo quanto disposto dagli artt. 78 e 79, è prevista la possibilità di far valere i propri diritti anche dinanzi all'**autorità giudiziaria dello Stato membro** in cui il titolare del trattamento o il responsabile hanno uno stabilimento.

Il ricorso al Garante non può tuttavia essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria, e la presentazione di un ricorso rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

Qualora l'interessato subisca **un danno materiale o immateriale** causato dalla **violazione del GDPR**, esso ha diritto ad ottenere **il risarcimento del danno** dal titolare del trattamento o dal responsabile.

Infatti, mentre il titolare del trattamento risponde sempre del danno cagionato nei confronti dell'interessato, il **responsabile del trattamento** ne risponde **esclusivamente** nel caso in cui **non** abbia **adempiuto agli obblighi** dello stesso Regolamento, diretti soltanto nei confronti del responsabile.

Entrambi i soggetti sono esonerati dalla responsabilità del danno cagionato soltanto nel caso in cui venga dimostrato che l'evento **non** sia in alcun modo a loro **imputabile**.
Per ottenere il risarcimento l'interessato è tenuto a rivolgersi all'autorità giudiziale.
Contro il provvedimento espresso o il rigetto tacito del ricorso, il titolare o l'interessato possono proporre **opposizione** con ricorso (che non sospende l'esecuzione del provvedimento).

Autorità giudiziaria ordinaria
Le **controversie** che riguardano l'applicazione delle disposizioni previste dal Regolamento, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'**autorità giudiziaria ordinaria**.

Sanzioni
Le seguenti tabelle forniscono una sintesi delle sanzioni per violazioni di natura amministrativa e penale.

	SANZIONE
- **VIOLAZIONI AMMINISTRATIVE**	Si tratta di **sanzioni** emesse da parte **del Garante**, per la quale il Regolamento dispone un tetto massimo del valore da attribuire a illeciti amministrativi, ovvero di importo **non superiore a 20 milioni di euro, mentre per le imprese non superiore al 4% del fatturato mondiale**. Nello specifico, a quanto deve ammontare la sanzione è un aspetto che il Legislatore comunitario rimanda a quello del singolo Paese. In Italia, il Legislatore non si è ancora pronunciato in merito. Tali violazioni prevedono **sanzioni più o meno pesanti** a seconda della **gravità** della violazione realizzata, dei soggetti coinvolti, del bene tutelato e alla natura dolosa o colposa della stessa violazione. In merito, l'art. 83 indica quelli che sono gli elementi considerati quando si deve infliggere una sanzione amministrativa pecuniaria: • la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; • il carattere doloso o colposo della violazione; • le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; • il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli artt. 25 e 32; • eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; • il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; • le categorie di dati personali interessate dalla violazione; • la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

	• qualora siano stati precedentemente disposti provvedimenti di cui all'art. 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti; • l'adesione ai codici di condotta approvati ai sensi dell'art. 40 o ai meccanismi di certificazione approvati ai sensi dell'art. 42; e • eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione. **Le sanzioni amministrative possono ammontare fino a 10 milioni, o fino al 2% del fatturato mondiale**, in caso di: • violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione; • trattamento illecito di dati personali che non richiede l'identificazione dell'interesato; • mancata o errata notificazione o comunicazione all'autorità competente; • violazione dell'obbligo di nomina del responsabile della protezione dei dati; • mancata applicazione della misura di sicurezza. **Le sanzioni amministrative pecuniaria può arrivare fino a 20 milioni di eur, al 4% del fatturato mondiale,** in casi di: • inosservanza di un ordine, limitazione provvisoria relativa ad un trattamento, imposti dall'autorità nazionale competente; • trasferimento illecito dei dati personali ad un Paese terzo.

12. La Privacy negli studi professionali

Anche i **professionisti** ricadono nell'ambito applicativo del Regolamento GDPR.

Pertanto, è necessario individuare le **misure di sicurezza necessarie** per garantire un'adeguata protezione dei dati personali trattati dal titolare del trattamento e da tutti i soggetti che a diverso titolo intervengono all'interno dello studio professionale.

Al fine di agevolare i professionisti nella corretta applicazione del nuovo GDPR, il Consiglio Nazionale Dottori Commercialisti ed Esperti Contabili e la Fondazione Nazionale dei commercialisti hanno recentemente pubblicato, sul Sito istituzionale, il documento "*Il Regolamento UE/2016/679 - General Data Protection Regulation (GDPR): nuove regole comunitarie e precisazioni in materia di protezione dei dati personali",* redatto dal "Gruppo di lavoro *Privacy*", contenente una *check-list* che permette di effettuare una sorta di autovalutazione preventiva della struttura di gestione dei dati personali applicata all'interno dello **studio professionale**, anche se non può considerarsi sufficiente ai fini del rispetto del principio dell'*accountability*.

13. Riferimenti
Normativi:

- Atto Governo 22/2018
- D.Lgs. 30 giugno 2003, n. 196
- Direttiva 95/46/CE

Prassi:

- Documento CNDCEC e FNC – Aprile 2018
- Garante per la Protezione dei dati personali, Provvedimento 22 maggio 2018
- Guida Garante Privacy 2018, febbraio 2018
- Linee Guida del gruppo di lavoro "Articolo 29"