AVVOCATO GILDA MUNNO
Intellectual Property Lawyer
mail:g.munno91@gmail.com

REGOLAMENTO N. 679/2016

NORMATIVACOMUNITARIA
E NUOVI ADEMPIMENTI IN MATERIA DI PRIVACY

AMBITO DI APPLICAZIONE ED APPROCCIO PRATICO

Cosa si intende con il termine privacy?

Ormai entrato nell'uso comune, il termine **privacy** indica il **diritto alla riservatezza** delle informazioni personali e della propria vita privata.

Le **normative per la privacy** che si sono susseguite negli ultimi anni sono state pensate per salvaguardare e tutelare la sfera privata del singolo individuo, impedendo che le informazioni riguardanti la sfera personale siano divulgate senza l'autorizzazione dell'interessato e che soggetti terzi si intromettano nella sfera privata. La tutela dei dati personali è ormai riconosciuto come un diritto dell'individuo ad avere il controllo sulle informazioni e sui dati riguardanti la sua vita privata, per il quale la legislazione deve fornire gli strumenti necessari.

Cosa è il diritto alla privacy?

L'istituto nasce negli Stati Uniti nel 1890 come diritto "a essere lasciato solo" (*to be let alone*) e viene elaborato in Italia dagli anni '60-'70 come generico diritto alla libera determinazione nello svolgimento della propria personalità.

Con il complicarsi della comunicazione elettronica e digitale, il concetto si è evoluto e oggi si parla di **privacy** non solo nel senso di **protezione dei dati personali** e come diritto di impedire la rilevazione di informazioni sul nostro conto. Con un'accezione più ampia, si intende infatti anche il diritto a esprimere liberamente le proprie aspirazioni, quindi l'autodeterminazione e la sovranità su se stessi, il riconoscersi parte attiva nel rapporto con le istituzioni e nel rispetto reciproco delle libertà.

Origini legislative in Europa

Dei primi riferimenti alla **privacy** si possono trovare nella **Convenzione europea dei diritti dell'uomo** del 1950 che stabiliva come non può esservi ingerenza di una autorità pubblica nell'esercizio del diritto alla propria libertà individuale, con l'eccezione di ingerenze previste dalla legge come misure necessarie per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui.

Questo fondamentale concetto è stato riportato e ampliato in successivi altri accordi internazionali, come quello di Schengen, e nella Carta dei diritti fondamentali dell'Unione europea che all'art. 8 recita:

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Origini legislative in Italia

La Costituzione italiana è nata in un tempo in cui il diritto alla privacy non era sentito, ma tra le sue righe si possono rintracciare numerosi riferimenti che anticipano le normative successive, ad esempio negli articoli 14, 15 e 21, rispettivamente riguardanti il domicilio, la libertà e segretezza della corrispondenza, e la libertà di manifestazione del pensiero. Tuttavia, un primo e importante accenno alla **privacy** è oggi visto nell'articolo 2 della Costituzione, che incorpora la privacy nei diritti inviolabili dell'uomo, come del resto ha sostenuto la Corte Costituzionale con la sentenza n. 38 del 1973.

Una prima elaborazione del **diritto alla privacy** la troviamo a livello giurisprudenziale, con la sentenza della Corte di Cassazione n. 4487 del 1956, che segue un ricorso degli eredi del tenore Enrico Caruso: questa identificava tale diritto nella tutela delle situazioni e vicende personali e familiari che, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile.

Un'affermazione di questo tipo ha fondato il bilanciamento tra **riservatezza** e diritto di cronaca: in quanto la linea di demarcazione tra privacy e diritto all'informazione di terzi è oggi data dalla popolarità del soggetto, pur precisando che anche soggetti famosi conservano tale diritto, limitatamente a fatti che non riguardano i motivi della popolarità.

L'Italia è arrivata come penultima in Europa ad approvare una **legge di tutela della privacy** di applicazione generale solo nel 1996 con la legge 675.

La **legge 675/1996** sulla **Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali** attuava la **Direttiva 95/46/CE** del Parlamento Europeo e del Consiglio, relativa alla tutela delle persone fisiche con riguardo al **trattamento dei dati personali** e alla libera circolazione di tali dati.

Qual è la legge sulla privacy?

Il **decreto 196 del 2003** "**Codice in materia di protezione dei dati personali**" detto anche "**Testo unico sulla Privacy**" o **Codice della privacy**, entrato in vigore dal 1° gennaio 2004, ha ampliato il percorso legislativo compiuto dall'Italia in materia di dati personali a partire dalla legge 675/96, chiarendo che la privacy non è solo il diritto a non vedere trattati i propri dati senza consenso, ma anche l'adozione di cautele tecniche e organizzative che tutti, comprese le persone giuridiche, devono rispettare per trattare in maniera corretta i dati altrui.

Tale normativa è considerata la più completa a livello europeo: dedica la prima parte ai principi generali, dettando le definizioni essenziali per la comprensione della normativa, tra le quali quelle di **dato personale** e di **trattamento**.

Per uniformare le normative sulla privacy nazionali e migliorare la **protezione dei dati personali** dei cittadini europei dentro e fuori l'Unione, il 4 maggio 2016 viene pubblicato in Gazzetta Ufficiale il **Regolamento UE 2016/679** del Parlamento Europeo e del Consiglio del 27 aprile 2016, cosiddetto **GDPR** (**General Data Protection Regulation**), in sostituzione della direttiva 95/46/CE.

In seguito all'entrata in vigore del **GDPR**, il testo del **codice della Privacy** è stato aggiornato con le modifiche apportate dal **Decreto di adeguamento al GDPR** **(Decreto Legislativo 10 agosto 2018, n. 101),** dal **D.M. 15 marzo 2019** e dal **D.L. 14 giugno 2019, n. 53.**

CHE COS'E' IL GENERAL DATA PROTECTION REGULATION?

- Dopo 4 anni di preparazione e dibattito è stato approvato il GDPR dal Parlamento Europeo il **27 aprile 2016**.

- Come prevede l'art. 99 il Regolamento si applicherà a decorrere dal **25 maggio 2018**.

- Il nuovo Regolamento Generale Europeo sulla Protezione dei Dati Personali n. 2016/679 (GDPR), con i suoi 99 articoli ha riscritto la disciplina della Privacy a livello europeo eliminando le differenze di approccio tra Stati membri .

- L'obiettivo è quello di definire una BASELINE per la protezione dei dati

- **OGGETTO**

Insieme di norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

- **AMBITO DI APPLICAZIONE**

Tutti i trattamenti automatizzati e non di dati personali, ad esclusione di:

- Attività extra UE;
- Politica estera e sicurezza commune;
- Finalità personali o domestiche;
- Prevenzione, indagine, accertamento reati, sicurezza pubblica

- **AMBITO DI APPLICAZIONE TERRITORIALE**

- Stabilimento del Titolare, Titolare o Responsabile del trattamento nell'UE;
- Titolare e Responsabile fuori dall'UE, qualora gli Interessati siano in UE, in caso di:
  a) Offerta di beni e serizi;
  b) Monitoraggio comportamento degli interessati.

DEFINIZIONI

Ai fini del regolamento per "**dato personale**" si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato");
si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Ai sensi dell'art. 4 «È vietato 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».

Trattamento: 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;

PRINCIPIO DI CORRETTEZZA, TRASPARENZA, LIMITAZIONE DELLE FINALITA'

- La **correttezza** del trattamento è essenzialmente legata all'idea che gli interessati devono essere consapevoli del fatto che i loro dati personali saranno trattati, compreso il modo in cui i dati saranno raccolti, conservati e utilizzati, per consentire loro di prendere una decisione informata.

- Il principio della **trasparenza** impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Il principio di Trasparenza non è direttamente spiegato nel GDPR, se ne fa maggiore chiarezza nell'Art. 12: «*in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato*».

- I Titolari devono innanzitutto identificare le particolari **finalità** per le quali i dati personali saranno trattati (by design)

Tali scopi diverranno i limiti entro i quali i dati personali devono essere raccolti e utilizzati dai responsabili del trattamento dei dati.

Il trattamento secondario può essere effettuato legalmente solo quando tale trattamento è considerato compatibile con lo scopo originale per il quale i dati personali sono stati raccolti

PRINCIPIO DI MINIMIZZAZIONE DEI DATI, ESATTEZZA e LIMITAZIONE DELLA CONSERVAZIONE

Il principio della "**minimizzazione dei dati**" indica che un Titolare del trattamento dei dati dovrebbe limitare la raccolta di informazioni personali a ciò che è direttamente rilevante e necessario per raggiungere uno scopo specifico.
Dovrebbero inoltre conservare i dati solo per il tempo necessario a raggiungere lo scopo.

I dati raccolti dovranno essere **esatti** e, se necessario, aggiornati.
Di conseguenza le Aziende dovranno adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente eventuali dati inesatti rispetto alle finalità per le quali sono trattati.

I dati dovranno essere sempre trattati in maniera da garantire una sicurezza adeguata, il che prevede l'adozione di misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

Il GDPR non stabilisce alcun periodo minimo o massimo per la **conservazione** dei dati personali ma non devono essere conservati per un periodo superiore a quello necessario per tale scopo o per tali finalità.

IL QUADRO NORMATIVO APPLICABILE IN ITALIA

Regolamento 2016/679	**IN VIGORE,** pienamente applicabile dal 25 maggio 2018
Direttiva 1995/46	**DECADE** il 24 maggio 2018
Codice D.Lgs. 196/2003	**IN VIGORE, NON DECADE**, viene coordinato con il reg. UE secondo i criteri indicati dalla Legge di Delegazione
Provvedimenti Autorità Garante	**IN VIGORE, NON DECADONO,** fino a quando non verranno modificati, sostituiti, abrogati
Accordi internazionali su trasferimento dati	**IN VIGORE, NON DECADONO,** fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissioni UE	**IN VIGORE, NON DECADONO,** fino a quando non verranno modificati, sostituiti, abrogati

PRIVACY BY DESIGN e PRIVACY BY DEFAULT

❖ Privacy by design

Approccio secondo cui le imprese devono predisporre i necessari strumenti di tutela (ad es. pseudonomizzazione) e protezione dei dati personali prima di iniziare il trattamento, con il fine di prevenire, più che correggere in un momento successivo, una possibile violazione.
E' necessaria una valutazione del rischio (*risk based approach*) prima di iniziare il trattamento

❖ Privacy by default

Le imprese dovrebbero trattare i dati personali nella misura necessaria e sufficiente per le finalità previste del trattamento e per il periodo strettamente necessario a tale scopo. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

La gestione dei dati personali non è più solo un adempimento ma diventa un processo aziendale che deve essere gestito modificando l'organizzazione delle imprese. Si va verso la predisposizione di un modello organizzativo della gestione dei dati personali finalizzato a prevenire i rischi di utilizzo illecito dei dati.

ACCOUNTABILITY

- E' il principio della "responsabilizzazione" di Titolari e Responsabili nel trattamento dei dati, che si sostanzia nell'adozione di comportamenti volti a dimostrare l'attuazione delle misure e tutele previste dal Regolamento.

- Il Regolamento intende spostare sui Titolari e Responsabili del trattamento la decisione circa le modalità, le garanzie e i limiti del trattamento.

- In particolare, il Titolare del trattamento deve mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare il grado di conformità delle attività di trattamento con il Regolamento.

- Il Titolare può dimostrare che il trattamento dei dati è conforme al Regolamento attraverso l'adozione di misure di sicurezza o l'adesione ai Codici di Condotta o meccanismi di certificazione (la cui predisposizione è fortemente incoraggiata dagli Stati membri, dalle Autorità di controllo e dalle Istituzioni Europee).

REQUISITI DI LEGITTIMITA’
E CONDIZIONI DI LICEITA’ DEL TRATTAMENTO

Il Regolamento individua i requisiti di legittimità del trattamento nella (i) Liceità, correttezza e trasparenza, (ii) Limitazione della finalità, (iii) Minimizzazione dei dati, (iv) Esattezza, (v) Limitazione della conservazione, (vi) Integrità e riservatezza.

Condizioni di liceità del trattamento:
Il trattamento è lecito solo se ricorre almeno una delle seguenti condizioni:

1. **Consenso** dell’Interessato (*l'interessato ha dato il consenso al trattamento dei propri dati personali per uno o più scopi specifi*ci).
2. **Obblighi contrattuali o precontrattuali**.
3. **Obblighi di legge** cui è soggetto il Titolare del trattamento.
4. **Interessi vitali** dell’Interessato o di terzi (Residuale rispetto alle altrecondizioni)(*il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica*).
5. **Interesse pubblico** o esercizio di pubblici poteri (*il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri conferiti al responsabile del trattamento*).
6. **Interesse legittimo** prevalente del Titolare del trattamento o di terzi cui i dati vengono comunicati a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell’Interessato.

CONSENSO

- Non è richiesta la forma scritta, ma il Titolare deve essere in grado di dimostrare che l'Interessato ha prestato il consenso.
- Per i dati sensibili il consenso deve essere esplicito.
- Può essere revocato in qualsiasi momento.

La richiesta di consenso deve essere:

- Chiara.
- Distinguibile dalle altre materie.
- Forma comprensibile e facilmente accessibile.
- Linguaggio semplice.

Minori:

- Consenso valido se il minore ha compiuto i 16 anni.

INFORMATIVA

L'**Informativa** presentata agli interessati deve essere:

» Concisa;
» Facilmente accessibile;
» Di facile comprensione.
» Linguaggio semplice e chiaro.

L'Informativa è fornita, in linea generale, per iscritto e in formato elettronico.
Possibile utilizzo di icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone devono essere visibili da dispositivo automatico

In caso di **raccolta dei dati presso l'Interessato**, l'Informativa dovrà indicare:

» I dati del Titolare del trattamento.
» Responsabile della protezione dei dati (RPD), se esistente.
» Finalità e base giuridica del trattamento.
» Interesse legittimo del Titolare o di terzi, se esistente.
» Destinatari dei dati.
» Intenzione di trasferire dati in un paese extra UE, se esistente.
» Periodo di conservazione dei dati.
» Diritti degli Interessati (accesso, rettifica, cancellazione, limitazione opposizione, portabilità).
» Diritto di revocare il consenso, se esistente.
» Diritto di proporre reclamo;.
» Conseguenze della mancata comunicazione dei dati, se esistente.
» Esistenza di processi decisionali automatizzati (anche profilazione).

L'informativa non è necessaria se e nella misura in cui l'interessato già dispone delle informazioni.

INFORMATIVA

Nel caso in cui i dati **NON** siano raccolti presso l'Interessato, l'Informativa dovrà avere il medesimo contenuto di quella presentata in caso di raccolta di dati presso l'Interessato, ad eccezione delle eventuali conseguenze della mancata comunicazione dei dati, con l'aggiunta di: (i) l'indicazione delle categorie dei dati oggetto del trattamento; (ii) la fonte da cui hanno origine i dati personali.

Tempi:

» L'informativa deve essere comunicata non oltre 1 mese dall'ottenimento dei dati.

Eccezioni:

» L'informativa non deve essere comunicata se:

1. L'Interessato già dispone delle informazioni.
2. Comunicazione impossibile/sforzo sproporzionato per il Titolare.
3. Ottenimento e comunicazione previsti da UE.
4. Segreto professionale.

DIRITTI DEGLI INTERESSATI

Nell'ambito del trattamento dei propri dati personali gli Interessati hanno i seguenti **diritti**:

- Diritto di accesso;
- Diritto alla rettifica;
- Diritto all'oblio (cancellazione);
- Diritto alla limitazione del trattamento;
- Diritto alla portabilità dei dati;
- Diritto di opposizione.

Il Titolare deve rispondere all'interessato entro 1 mese dall'esercizio di uno dei diritti sopra indicati.

Obbligo di notifica delle eventuali rettifiche, cancellazioni o limitazioni ai destinatari cui sono stati comunicati i dati.

Le informazioni fornite, e l'esercizio dei diritti, sono gratuite salvo il caso di richieste infondate, eccessive o ripetitive per cui può essere previsto un contributo economico

DIRITTO DI ACCESSO, DIRITTO DI RETTIFICA, DIRITTO DI OPPOSIZIONE

DIRITTO DI ACCESSO

Diritto ad ottener e la conferma circa l'esistenza del trattamento nonché l 'accesso a specifiche informazioni relative al trattamento dei dati.
Diritto di richiedere una copia delle informazioni.
E' incentivata la possibilità di consultare i dati direttamente da remoto.

DIRITTO DI RETTIFICA

Diritto di ottenere la rettifica e l'integrazione dei propri dati personali

DIRITTO DI OPPOSIZIONE

Diritto di opporsi al trattamento per motivi derivanti dalla situazione particolare dell'interessato.
Diritto di opporsi, in qualsiasi momento, al trattamento effettuato per finalità di telemarketing, compresa la profilazione

DIRITTO ALL'OBLIO (CANCELLAZIONE)

- Diritto di ottenere la cancellazione dei propri dati personali e conseguente obbligo del Titolare del trattamento di procedere nelle seguenti ipotesi:
- Dati non più necessari rispetto alle finalità del trattamenti.
- Revoca del consenso su cui si basa il trattamento.
- Opposizione al trattamento.
- Dati trattati illecitamente.
- Dati da cancellare per adempiere ad un obbligo di legge.
- Dati raccolti per l'offerta di servizi per la società dell'informazione.

- Obbligo per il Titolare di informare gli altri Titolari della richiesta dell'Interessato di cancellarli.

Il Diritto all'oblio **NON si applica** per:

- L'esercizio del diritto alla libertà di espressione e di informazione.
- Adempimento di un obbligo legale o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.
- motivi di interesse pubblico nel settore della sanità pubblica.
- fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.
- accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

- ✓ Diritto più esteso rispetto al blocco del trattamento ai sensi dell'art. 7 comma 3 lett. a) del D.Lgs. 196/2003.

- ✓ L'Interessato può ottenere la limitazione del trattamento se:
  A. contesta l'esattezza dei dati, per il periodo necessario al Titolare del trattamento per effettuare la verifica;
  B. trattamento illecito e richiesta di limitazione;
  C. dati necessari per l'esercizio in sede giudiziaria;
  D. opposizione dell'Interessato in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'Interessato.

- ✓ Il dato personale oggetto della limitazione dovrà essere "contrassegnato", in attesa delle successive determinazioni, attraverso idonei strumenti (anche elettronici).

DIRITTO ALLA PORTABILITÀ DEI DATI

Diritto dell'Interessato di ricevere dal Titolare i propri dati, in formato leggibile da dispositivo automatico, e di trasferirli ad altro Titolare, a condizione che:

- il trattamento si basi sul consenso o su un contratto;
- il trattamento sia eseguito con mezzi automatizzati (no cartaceo);
- il trattamento abbia ad oggetto dati "forniti" dall'Interessato.

Se richiesto dall'Interessato e tecnicamente possibile il Titolare deve essere in grado di garantire il trasferimento diretto dei dati al nuovo Titolare del trattamento.

E' opportuno che il Titolare utilizzi un formato dei dati interoperabile, così da poter garantire agevolmente l'eventuale trasferimento.

TITOLARE DEL TRATTAMENTO

- Il Titolare del trattamento "*mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*" (Accountability). L'adesione a Codici di Condotta o meccanismi di certificazione costituisce un elemento idoneo a rappresentare il rispetto del Regolamento.

- Possibile **contitolarità del trattamento**. In tale ipotesi i contitolari dovranno disciplinare per iscritto i rispettivi compiti e responsabilità, con particolare riguardo all'esercizio dei diritti degli Interessati.

- Il Titolare (o il Responsabile) che si trovi fuori UE dovrà nominare un Rappresentante all'interno dell'UE che costituirà l'interlocutore diretto per le Autorità di controllo e gli Interessati.

RESPONSABILE DEL TRATTAMENTO

- Il Responsabile del trattamento deve essere nominato tra coloro che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a quanto previsto nel Regolamento.

- Può nominare un altro Responsabile previa autorizzazione scritta del Titolare, ma resta responsabile di possibili inadempimenti del sub-Responsabile.

- Deve essere incaricato attraverso un contratto che preveda espressamente "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 Regolamento individua inoltre ulteriori obblighi del Responsabile che devono essere indicati nel contratto

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Regolamento introduce la figura del **Responsabile della Protezione dei Dati** (RPD) il quale ha il compito di svolgere attività che non si limitano al mero controllo formale circa il livello di protezione dei dati, ma si estendono al supporto strategico alle decisioni operative del Titolare. E' un vero e proprio manager del trattamento dei dati (o privacy designer).

Il Titolare e il Responsabile del trattamento nominano il RPD nei seguenti casi:

1. trattamento effettuato da un'Autorità pubblica o organismo pubblico;
2. trattamenti che, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
3. le attività principali del Titolare o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali (dati sensibili) o di dati relativi a condanne penali e a reati.

Possibilità di nominare un unico RPD nell'ambito di un Gruppo di imprese.
Il RPD è designato tra i dipendenti del Titolare o Responsabile del trattamento ovvero tra professionisti terzi, in funzione delle sue qualità professionali, con particolare riferimento alla conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il RPD deve essere **autonomo ed indipendente**.

E' tempestivamente e costantemente coinvolto dal Titolare e dal Responsabile in tutte le questioni relative al trattamento.

Il Titolare ed il Responsabile del trattamento forniscono al RPD le **risorse necessarie** per assolvere i compiti assegnatigli e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Il RPD riferisce direttamente al vertice gerarchico del Titolare o del Responsabile del trattamento.

Gli Interessati possono contattare il RPD per tutte le questioni attinenti al trattamento.

Obbligo di segretezza e possibilità di svolgere attività diverse purché non vi sia conflitto di interessi.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il RPD è incaricato di eseguire ALMENO i seguenti compiti:

1. **informare** e fornire consulenza al Titolare o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi di legge relativi alla protezione dei dati;
2. **verificare** il rispetto della normativa applicabile nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
3. **fornire**, se richiesto, un parere in merito alla Valutazione d'Impatto e sorvegliarne lo svolgimento;
4. **cooperare** con l'Autorità di controllo;
5. fungere da **punto di contatto** per l'Autorità di controllo per questioni connesse al trattamento.

REGISTRO DELLE ATTIVITA'

Il Titolare ed il suo rappresentante devono tenere un Registro delle Attività in cui sono elencati i trattamenti svolti ed indicate le seguenti informazioni:

I. Dati di contatto del Titolare del trattamento.
II. Finalità del trattamento.
III. Descrizione delle categorie di Interessati e dei dati personali.
IV. Eventuale trasferimento dei dati verso paesi extra UE.
V. Termini ultimi per la cancellazione dei dati.
VI. Descrizione delle misure di sicurezza tecniche e organizzative applicate al trattamento.

Il Responsabile ed il suo rappresentante devono tenere un Registro di tutti i trattamenti svolti per conto di un Titolare del trattamento, che riporti le seguenti informazioni:

I. Dati di contatto del Responsabile e del Titolare del trattamento e suo rappresentante per conto del quale è effettuato il trattamento.
II. Le categorie dei trattamenti effettuati per conto di ogni Titolare.
III. Eventuale trasferimento di dati verso paesi extra UE.
IV. Descrizione delle misure di sicurezza tecniche e organizzative.

REGISTRO DELLE ATTIVITA'

I Registri sono tenuti in **forma scritta** (anche in formato elettronico).

L'obbligo della tenuta del Registro:

SI

SI applica alle imprese con un numero di dipendenti uguale o maggiore di 250

NO

NON si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano (i) possa presentare un rischio per i diritti e le libertà dell'Interessato, (ii) il trattamento non sia occasionale o includa il trattamento di dati sensibili, o i dati personali relativi a condanne penali e a reati

SICUREZZA DEL TRATTAMENTO

Il Titolare e il Responsabile del trattamento mettono in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ed in particolare, inter alia:

- la pseudonimizzazione e la cifratura dei dati personali;
- la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare il livello di sicurezza si tiene conto di dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

VIOLAZIONE DEI DATI PERSONALI

- ✓ Il Titolare, anche informato dal Responsabile del trattamento, notifica la violazione all'Autorità di controllo entro **72 ore** da quando ne è venuto a conoscenza, salvo che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
- ✓ Il Titolare del trattamento notifica la violazione all'Interessato qualora essa sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
- ✓ In ogni caso non è richiesta la notifica all'Interessato qualora:
- ✓ Il Titolare ha adottato misure di protezione dei dati adeguate.
- ✓ Il Titolare ha messo in atto, successivamente, misure adeguate a protezione da possibili rischi elevati.
- ✓ La comunicazione richiederebbe sforzi sproporzionati.

VALUTAZIONE DI IMPATTO

Se il trattamento presenta un rischio elevato per i diritti e le libertà delle persone, il Titolare, consultandosi con il Responsabile del trattamento, deve preliminarmente effettuare una Valutazione di Impatto dei trattamenti sulla protezione dei dati.

La **Valutazione di Impatto** è sempre richiesta nei seguenti casi:

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

La Valutazione di impatto **deve contenere**:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

Qualora la Valutazione d'Impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio, quest'ultimo, prima di procedere al trattamento, deve consultare l'Autorità di controllo.

TRAFERIMENTO DI DATI VERSO PAESI EXTRA UE O ORGANISMI INTERNAZIONALI

⇒ Il trasferimento può essere effettuato se lo Stato terzo (extra UE) o l'Organizzazione ha superato la decisione di adeguatezza della Commissione Europea.
⇒ In mancanza di una decisione di adeguatezza, il Titolare o il Responsabile può trasferire i dati solo se ha fornito garanzie adeguate e a condizione che gli Interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.
⇒ E' incoraggiata l'adozione, da parte delle Autorità di controllo, di norme vincolanti di impresa da utilizzare per lo scambio di dati all'interno di gruppi di imprese con sedi anche in paesi extra UE.
⇒ Divieto di trasferire dati in un paese extra UE sulla base di decisioni giudiziarie o amministrative, salvo che esista un accordo bilaterale.
⇒ Possibilità di trasferire i dati verso paesi extra UE ed organismi internazionali anche in assenza di una decisione di adeguatezza o garanzie adeguate, in base a delle ipotesi specifiche indicate nel Regolamento.

RECLAMO ALL'AUTORITÀ DI CONTROLLO E RICORSO GIURISDIZIONALE

Ogni Interessato ha diritto di proporre:

1) reclamo all'Autorità di controllo competente nello Stato membro in cui ha la residenza ovvero nel luogo in cui si è verificata la violazione, qualora il trattamento che lo riguarda violi il Regolamento;

2) ricorso giurisdizionale, dinanzi alla competente Autorità Giudiziaria, nei confronti del Titolare o Responsabile del trattamento, qualora ritenga che i diritti di cui gode a norma del Regolamento siano stati violati a seguito di un trattamento;

3) ricorso giurisdizionale (azionabile da qualsiasi persona fisica o giuridica), dinanzi alla competente Autorità Giudiziaria, avverso una decisione giuridicamente vincolante dell'Autorità di controllo che la riguarda nonché in caso l'autorità di controllo non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto.

SANZIONI AMMINISTRATIVE

- Le sanzioni amministrative irrogate dalle Autorità di controllo devono essere, in ogni singolo caso, effettive, proporzionate e dissuasive.
- Il Regolamento individua gli elementi da prendere in considerazione per l'applicazione della sanzione amministrativa.
- Le sanzioni applicabili, individuate nel Regolamento, sono pari a:

I. fino ad Euro 10.000.000,00, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni degli obblighi relativi a: minori, obblighi del Titolare e Responsabile, obblighi dell'organismo di certificazione, obblighi dell'organismo di controllo;

II. fino ad Euro 20.000.000,00, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni degli obblighi relativi a: principi di base del trattamento, comprese le condizioni relative al consenso, diritti degli interessati, trasferimento dati a paese extra UE, obblighi imposti dagli stati membri per specifiche categorie – anche in ambito lavorativo − l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

III. Le sanzioni amministrative pecuniarie sono inflitte in aggiunta alle, o in luogo delle, sanzioni di cui all'art. 58 par. 2 lett. da a) a h) e j) del Regolamento (ad es. avvertimenti, ammonimenti, ingiunzioni, limitazioni ai trattamenti, ordine di cancellazione, rettifica o limitazione del trattamento, revoca della certificazione o ingiunzione all'Organismo certificatore di ritirare o non emettere la certificazione, ordine di sospensione dei flussi di dati verso un destinatario).

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
Fino a **10.000.000 EUR** o, per le imprese, fino al **2%** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. 8	Verifica che il consenso del trattamento sia prestato o autorizzato dal titolare della responsabilità genitoriale nel caso di offerta diretta di servizi della società dell'informazione a minori di età inferiore ai 16 anni.
	Art. 11	Obbligo di non conservazione, acquisizione o trattamento di informazioni per identificare l'Interessato se le finalità del trattamento non richiedono o non richiedono più l'identificazione dell'Interessato.
	Art. 25	Adozione di misure tecniche e organizzative atte ad attuare i principi di protezione dei dati, la tutela dei diritti degli Interessati e la garanzia che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento (c.d. *privacy by design e by default*).
	Art. 28	Designazione del Responsabile del trattamento e rispetto degli obblighi e compiti posti a carico del Responsabile.

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
Fino a **10.000.000 EUR** o, per le imprese, fino al **2%** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. 30	Tenuta dei Registri delle attività di trattamento.
	Art. 32	Adozione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio
	Art. 33 - 34	Notifica delle violazioni all'Autorità di controllo e all'Interessato.
	Art. 35 e 36	Obbligo di procedere alla valutazione di impatto ed alla successiva consultazione, ove richiesto dal Regolamento.
	Art. 37 - 39	Prescrizioni in tema di designazione del Responsabile della protezione dei dati (*Data Protection Officer*).

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
Fino a **20.000.000 EUR** o, per le imprese, fino al **4%** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. 5	Rispetto dei principi applicabili al trattamento liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
	Art. 6	Rispetto delle condizioni di liceità del trattamento.
	Art. 7	• Dimostrazione della prestazione del consenso e del rispetto delle condizioni per il consenso. • Tutela del diritto dell'Interessato di revoca del consenso.
	Art. 9	Rispetto delle condizioni di liceità del trattamento di categorie particolari di dati personali.

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
Fino a **20.000.000 EUR** o, per le imprese, fino al **4%** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. da 12 a 22	• Obblighi informativi nei confronti dell'Interessato. • Tutela dei diritti dell'Interessato (diritto d'accesso; di rettifica; all'oblio; di limitazione del trattamento; di notifica in caso di rettifica o cancellazione dei dati o limitazione del trattamento; alla portabilità dei dati; di opposizione; alla profilazione consenziente).
	Art. da 44 a 49	Obblighi connessi al trasferimento dei dati personali verso Paesi terzi o organizzazioni internazionali.
	Cap IX	Qualsiasi obbligo previsto dalle legislazioni degli Stati membri per specifiche situazioni di trattamento a norma del Capo IX del Regolamento.
	Art. 58	Rispetto di un ordine, di una limitazione di trattamento o di un ordine di sospensione di flussi di dati dell'Autorità di controllo o di un negato accesso ai sensi dell'Art, 58, par. I.