GDPR: Adempimenti per Professionisti e Imprese

dott. ing. Giuseppe Deleonibus

OPERA Professioni - Molfetta (BA)

Privacy Officer e Consulente Privacy

Socio Promotore FEDERPRIVACY n° AF101056

Se vi è materia tanto trasversale e complessa da interessare ampie fasce di categorie professionali, questa è diventata negli ultimi anni la protezione dei dati personali, che per abitudine e brevità si è ormai definire «**privacy**».
E con l'entrata in vigore del nuovo **Regolamento UE 2016/679** complica ulteriormente la vita dei professionisti, che sono chiamati ad un cambio di prospettiva, in quanto la nuova normativa non trova più applicazione solo in Italia, ma in tutti i Paesi dell'Unione Europea, con l'obiettivo di regolamentare uniformemente l'economia digitale, che comporta ormai quotidianamente **trasferimenti di dati personali** da una nazione all'altra, sia all'interno che al di fuori della UE.

Se da una parte fioriscono anche in Italia gli specialisti della data protection, i c.d. «**privacy officer**», che oltreoceano esistono dagli anni ‘90, ciò non esenta moltissimi altri professionisti focalizzati su altri rami dalla necessità di possedere preparazione e conoscenza in ambito privacy, **non potendo più relegare le tematiche della protezione dei dati a un insieme di moduli da produrre, come se si trattasse di un mero aspetto burocratico e superfluo**.

In primo luogo perché non c'è praticamente più alcun settore che non sia stato toccato da **informatizzazione** e **digitalizzazione**, che veicolano e moltiplicano i trattamenti di dati personali a dismisura rispetto a qualche anno fa. Di conseguenza, qualsiasi sia il cliente che il professionista curi e assista, si troverà sempre e puntualmente di fronte a criticità e adempimenti riguardanti la privacy da gestire diligentemente per evitare rischi di pesanti **sanzioni**, che **con il regolamento Europeo potranno arrivare fino a 20 milioni di euro a al 4% del fatturato annuo globale del trasgressore**.

Il secondo fattore che fa della privacy una tematica attuale di interesse per una larga platea di professionisti, è che questa è classificata come un'attività pericolosa ai sensi dell'**art. 2050 c.c.,** il quale stabilisce che «***Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno***».

E, lungi dall'essere un concetto esistente solo nel nostro diritto nazionale, quello del risarcimento per chi sia vittima di una violazione sui propri dati personali è riaffermato e scolpito nell'**art. 82 del GDPR**, nel quale è prescritto che «***Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento***».

Ecco perché la privacy non è materia per i soli cultori, ma si estende coercitivamente anche ai **Consulenti del Lavoro**, che per la natura della loro professione sono ‘circondati’ dai dati sensibili dei lavoratori, come quelli relativi allo stato di salute, e pure ai **Commercialisti**, che anche per un semplice otto per mille devono tenere in conto gli impatti privacy. E neppure un qualsiasi **Avvocato** sarà risparmiato dalla necessità di conoscere la materia ed essere dovutamente preparato: basterebbe, ad esempio, un banale errore di superficialità in una notifica o nella produzione di prove in giudizio, per causare dei gravi danni che, legge alla mano, sarebbe tenuto a risarcire di tasca propria.

Il GDPR è chiaro nella sua semplicità: **trattare un dato è un'operazione che va pianificata in anticipo, con norme, ruoli e documenti interni alle aziende idonei allo scopo**.

Professionista a prova di GDPR

dott. ing. Giuseppe Deleonibus

Nell’attività quotidiana dello **studio professionale**, il professionista si trova a gestire **dati particolarmente “*sensibili*”**, ossia informazioni che, secondo l’approccio interpretativo del GDPR, **meritano una protezione più elevata**, in quanto dalla loro diffusione illecita potrebbero derivare danni ingenti ai clienti e ai loro diritti. A tal fine, **alcuni dati vengono appositamente individuati come “*particolari*”**. Sono dati che devono essere protetti esattamente come gli altri, sia chiaro, ma che, per la loro natura, richiedono una maggiore attenzione e, in alcuni casi, un **rafforzamento di tale protezione**.

L’attività “tipica” di uno studio di **dottori commercialisti**, ad esempio, comporta il trattamento quasi quotidiano di **dati particolarmente “sensibili”**.

Si pensi, tanto per fare qualche esempio, a dati relativi a **spese mediche** (e relative visite effettuate, o patologie correlabili), a versamenti a favore di **comunità religiose**, a informazioni correlate a **infortuni** o a dati che possano evidenziare spiacevoli **vicende giudiziarie** o, addirittura, **condanne**.

Poniamo il caso che il professionista raccolga e tratti i dati personali esclusivamente per la finalità connessa al servizio richiesto dal cliente, quindi ad esempio il **Commercialista** per fornire consulenza in materia contabile o fiscale ai propri clienti, l'**Avvocato** per curare la difesa in giudizio, redigere contratti o pareri, il **Consulente del Lavoro** per amministrare le pratiche in materia di diritto del lavoro di un' impresa cliente, l'**Ingegnere Edile** per curare progetti ad esempio nel settore della domotica

Una delle prime operazioni da compiere è quella di controllare che il trattamento sia fondato sui principi del GDPR, principi di **liceità**, **correttezza**, **trasparenza** e quindi, è opportuno verificare che i **dati raccolti e trattati** siano esclusivamente **quelli strettamente necessari**, **pertinenti e adeguati a svolgere la finalità per cui sono richiesti**, **che siano adottate misure per aggiornarli o rettificarli tempestivamente al bisogno**, **che siano conservati per il tempo necessario ad espletare l'incarico conferito** (salvo il tempo ulteriore necessario a rispettare le norme amministrative), **che siano adeguatamente protetti**.

Se più professionisti operano all'interno del medesimo studio, si dovrà verificare se alla propria compagine organizzativa si applichi l'**art. 26 del GDPR** e quindi se i professionisti operano in qualità di **contitolari del trattamento**, determinando di comune accordo modalità e finalità del trattamento dei dati (in tal caso si dovrà sottoscrivere un accordo interno in cui i professionisti disciplinano le proprie responsabilità e obblighi in materia di dati personali) oppure se diversamente per essi operano gli artt. 28 e 29 e quindi se i collaboratori dello studio gestiscono dati personali per conto di un titolare che fissa finalità e modalità del trattamento, in tal caso, infatti sarà necessario designare, anche qui mediante opportuni contratti, tali collaboratori, responsabili del trattamento e lo stesso si dovrà fare con il fornitore del servizio di hosting, sul quale è alloggiato l'eventuale sito web e su cui transitano le email e con l'eventuale consulente IT che si occupa di aggiornare o manutenere il software gestionale dello studio (magari concesso in licenza) e con tutti gli altri eventuali soggetti cui si trasferiscono dati di clienti o collaboratori fuori dallo studio (si pensi ad esempio a coloro che forniscono il servizio di fatturazione elettronica in outsourcing), mentre i segretari dovranno essere designati incaricati del trattamento o comunque autorizzati a gestire i dati (e quei soli dati, utilizzando ad esempio il sistema dei "permessi") limitatamente a ciò che ad essi compete; a segretari e collaboratori dovranno essere impartite, inoltre, istruzioni operative o linee guida su come gestire i dati di terzi e proteggerli.

Dotazione dello studio

Lo studio dovrà poi dotarsi di **strumenti tecnici e organizzativi** adeguati e proporzionati al tipo di dati trattati, alla finalità del trattamento, alle modalità, al contesto organizzativo e ai rischi potenziali che il trattamento può provocare sui diritti e le libertà degli interessati, misure che consentano di garantire, l'integrità dei dati personali trattati, la disponibilità, la resilienza dei sistemi usati e un elevato grado di protezione dei dati stessi (cfr. art. 32 GDPR), in particolare, di quelli che transitano sui vari device (pc, smartphone, tablet, wi-fi)

Impiegare meccanismi che permettano di evitare accessi abusivi ai dati, alterazioni o modifiche degli stessi, cancellazioni, divulgazioni non autorizzate o violazioni di altro tipo

Firewall

Password

Protocolli SSL

Particolarmente, importante per il transito dei dati è l'uso di chiavette USB dotate di password o anche chiavette che consentono di **criptare i dati** ivi contenuti (il GDPR, infatti all'art. 32 consiglia proprio l'impiego di strumenti che consentano di cifrare i dati o comunque usare la pseudonimizzazione). Occorrerà poi ricorrere a strumenti che permettano di effettuare il back up, meglio se continuo dei dati, come ad esempio potrebbe essere un servizio di ***cloud*** fornito da un soggetto terzo di cui sarà necessario vagliare l'affidabilità e il grado di sicurezza offerto prima di sottoscrivere il contratto, designando, tra l'altro, anch'esso, responsabile del trattamento.

Fondamentale è anche il fatto di **mantenere i sistemi operativi sempre aggiornati** e i vari programmi e le applicazioni utilizzate, determinando, a priori, una manutenzione periodica; si consiglia inoltre di controllare i vari devices, come smartphone o tablet, impostando una limitazione all'uso dei dati contenuti, se su di essi sono conservati o transitano in qualche modo anche dati relativi a clienti. Il GDPR, peraltro, lo si ricorda, all'art. 32, lett. d, prevede l'**impiego di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento**.

Si tenga poi presente che anche il professionista, in qualità di titolare del trattamento (o contitolare, mentre il responsabile dovrà comunicare un'eventuale violazione al titolare) è chiamato a **comunicare al Garante eventuali violazioni sui dati personali entro 72 ore dal momento in cui ne viene a conoscenza**, pertanto, occorrerà pensare anche a procedure preventive che consentano di intervenire velocemente sulla violazione e procedere tempestivamente alla comunicazione all'autorità.

Persone fisiche e persone giuridiche

Il Considerando n. 14 del Regolamento, con riferimento ai dati trattati, precisa innanzitutto come sia opportuno applicare una vera e propria "protezione" ai dati, e come tale protezione si applichi alle **persone fisiche** (a prescindere dalla nazionalità o dal luogo di residenza) in relazione al trattamento dei loro dati personali.
È interessante il fatto che il Regolamento non disciplini il trattamento dei dati personali relativi a **persone giuridiche**. In particolare, precisa il Considerando citato, ci riferiamo a quei dati relativi a imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

Utili sono anche, per il nostro contesto, i principi contenuti nel Considerando n. 15, dove è precisato che la protezione delle persone fisiche si deve applicare sia al trattamento "**automatizzato**" sia al trattamento "**manuale**" dei dati personali (se i dati personali sono contenuti o destinati a essere contenuti in un archivio). **Non dovrebbero, allora, rientrare nell'ambito di applicazione del Regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine**.

VALUTAZIONE DI IMPATTO (ART. 35 GDPR)

Cosa è?	Procedura per valutare necessità e proporzionalità di un trattamento
Perché?	La DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. (WP 29 suggerisce di attuarla su TUTTI i trattamenti e non solo dove obbligatorio)
Quando?	PRIMA di procedere al trattamento RIESAME CONTINUO a intervalli regolari
Chi?	La responsabilità è SEMPRE del Titolare DPO collabora CSO/ CIO vengono consultati (se trattamento di tipo informatico)

È possibile operare utilizzando risorse competenti interne all'azienda oppure avvalersi di professionisti esterni esperti nelle problematiche privacy.
Normalmente, almeno per il primo assessment, è consigliato avvalersi di risorse esterne esperte in modo da inquadrare velocemente i metodi e le azioni da intraprendersi e pervenire in breve tempo ad una base dati completa.
Ricordiamoci che **l'assessment rappresenta di solito uno strumento preventivo gestito dall'azienda stessa che decide di monitorare un determinato fenomeno**.

I metodi sono i medesimi dell'**audit** che rappresenta uno strumento per valutare l'idoneità del sistema a determinate norme.

Un PIA è disegnato per raggiungere normalmente tre obiettivi:

- **Garantire la conformità con le normative**, e requisiti di politica legali applicabili per la privacy;
- **Determinare i rischi e gli effetti** che ne conseguono;
- **Valutare le protezioni e eventuali processi alternativi** per mitigare i potenziali rischi per la privacy.

Non rappresenta quindi un mero strumento atto a censire, ma diventa l'elemento più importante per affermare di essere conformi alle prescrizioni del Regolamento.

QUANDO È OBBLIGATORIA?

❖ Trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ad esempio:

- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

PIA (Privacy Impact Assessment): lo strumento base per censire i rischi privacy

non obbligatorio per aziende sotto i 250 dipendenti, è il documento che descrive i flussi di dati all'interno delle aziende e i relativi rischi per i dati.

Il cons. n. 91 esclude l'obbligatorietà della valutazione d'impatto sulla protezione dei dati solo per singoli professionisti, quali il singolo avvocato o medico

IL REGISTRO DELLE ATTIVITÀ TRATTAMENTO DEI DATI

Nell'affrontare questo tema è doveroso utilizzare una corretta terminologia. Si parla infatti di attività di trattamento e non di trattamenti, in quanto questi ultimi sono ben definiti dall'articolo 4 del GDPR che così li declina:

*«**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.*

Il Regolamento Europeo 2016/679 prevede, all'**art. 30**, un importante strumento di compliance aziendale, in materia di dati personali: **il registro delle attività di trattamento dei dati personali**.

Tenuto anche in formato elettronico dal Titolare del trattamento dei dati, tale registro **dovrà essere messo a disposizione dell'Autorità Garante** qualora lo richieda, così come è previsto dal par. 4 dell'art. 30: *"su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento **mettono il registro a disposizione dell'autorità di controllo**"*.

Quanto ai registri, si parla di registri al plurale, perché i documenti in questione sono due:

1) il **registro del titolare del trattamento**;
2) il **registro del responsabile del trattamento**.

Il registro del responsabile del trattamento riguarda le attività relative al trattamento svolte per conto di un titolare del trattamento.

COSA DEVE CONTENERE

- **Il nome e i dati di contatto del titolare del trattamento** e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- Le **finalità** del trattamento;
- La descrizione delle **categorie di interessati** e delle **categorie di dati personali**;
- Le **categorie di destinatari** a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- Se presenti, i **trasferimenti di dati personali verso paesi terzi** e la loro identificazione;
- I **termini ultimi** previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.

CHI DEVE DOTARSI

L'obbligo di redazione e adozione del registro non è generale: infatti il par. 5 dell'art. 30 specifica che esso non compete *"alle imprese o organizzazioni* ***con meno di 250 dipendenti****, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10"*.

I registri dei trattamenti

Fra gli altri compiti, il titolare e il responsabile del trattamento devono redigere i registri delle attività e dei trattamenti effettuati.
Formalmente la tenuta del registro rappresenta il sostituto della comunicazione diretta delle medesime informazioni al Garante della Privacy. È presumibile pensare che nel prossimo futuro, come già avvenuto per i dati forniti all'Agenzia delle Entrate per via telematica, anche per tali informazioni avverrà un processo analogo.
In realtà i registri da conservare e mantenere sono due:
- Il registro del titolare del trattamento, che contiene:
  - Anagrafica del titolare stesso, di un contitolare se presente, del rappresentante e del titolare alla protezione dati;
  - Le finalità del trattamento;
  - Le categorie degli interessati a cui fa capo il dato;
  - Eventuali termini per la cancellazione automatica del dato;
  - Un'eventuale descrizione generale delle misure di sicurezza tecnico-organizzative.
- Il registro del responsabile del trattamento, in cui sono presenti:
  - L'anagrafica dei responsabili del trattamento;
  - La descrizione delle categorie di trattamento effettuati;
  - Opzionalmente la descrizione delle misure di sicurezza intraprese.

La conservazione può avvenire in forma cartacea ma anche in forma elettronica rendendo sempre disponibile
il dato ad eventuali ispezioni dell'autorità garante.
È bene che il software aziendale adottato per gestire il progetto Privacy integri la gestione dei registri derivandoli direttamente dalla normale operatività.

INFORMATIVA

Tra i diritti si segnala quello all'**informativa**, per la quale il Garante per la protezione dei dati ha
formulato la seguente regola:

"*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*".

Trasparente

Intelligibile

In forma concisa

Informativa, come?

Linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori

Facilmente accessibile

Se si trasferisce i dati personali in **Paesi terzi**

Il **periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo

Il diritto di presentare un r**eclamo all'autorità di controllo**

La **base giuridica** del trattamento

Informativa, cosa deve contenere?

Se il trattamento comporta **processi decisionali automatizzati**

I **contatti del DPO** (se presente)

RACCOLTA DEL CONSENSO

Uno dei diritti più importanti correlati al tipo di dato, ossia il **consenso**, è ben delineato, nel suo senso più profondo, dal Considerando n. 32. La norma dice, infatti, che **il consenso deve essere espresso mediante un atto positivo inequivocabile attraverso il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile (appunto) di accettare il trattamento dei dati personali che lo riguardano**, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Al contrario, non dovrebbe configurare consenso il **silenzio**, l'**inattività** o la **preselezione di caselle**.

Si aprono spazi maggiori per la raccolta di un consenso manifestato attraverso i comportamenti positivi dell'interessato.

Sono in ogni caso illegittimi i consensi raccolti con caselle prebarrate.

COSA DEVONO FARE I PROFESSIONISTI/LE IMPRESE?

Le imprese **devono verificare se i consensi raccolti rispettino la disciplina** che diventerà operativa il 25 maggio 2018:

- se la risposta è **affermativa**, non dovranno adottare misure particolari e potranno proseguire i loro trattamenti;
- se invece la risposta è **negativa**, dovranno programmare gli interventi necessari per rendersi conformi con la normativa regolamentare europea.

DATA PROTECTION OFFICER

Articoli 37-38-39 GDPR

Il RGPD riconosce nel RPD uno degli elementi-chiave all'interno del nuovo sistema di *governance* dei dati.

dott. ing. Giuseppe Deleonibus

Il DPO è obbligatorio:

1) Se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico.

2) Se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala.

3) Se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Cosa si intende per “Attività principali”

Con “attività principali” si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento.

Considerando 97 - . .
le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria.

Cosa si intende per “Larga Scala”

INDICATORI:

- Il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- Il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- La durata, ovvero la persistenza, dell’attività di trattamento;
- La portata geografica dell’attività di trattamento.

Considerando 91 - . .
larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presen-tano un rischio elevato . . . .

Il **WP29** individua alcune casistiche di trattamenti su "**larga scala**". Esse sono:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici telematici.

Non sono considerati su “Larga Scala”:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

QUALITÀ PROFESSIONALI DEL DPO

ART. 37 COMMA 5

Il Titolare deve fornire le risorse necessarie al DPO per mantenere la propria conoscenza specialistica (Vedi art. 38, comma 2).

Il Responsabile della protezione dei dati personali, al quale **non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi**, deve:

- possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento;
- poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare;
- agire in piena indipendenza (considerando 97 del Regolamento UE 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici;
- poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.

Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, Garante della Privacy, 29.03.2018

CHI SONO I SOGGETTI PRIVATI OBBLIGATI ALLA SUA DESIGNAZIONE?

Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679. Si tratta di **soggetti le cui principali attività** (in primis, le attività c.d. di "core business") **consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati** (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", v. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4).

Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, Garante della Privacy, 29.03.2018

Sono tenuti alla nomina, a titolo esemplificativo e non esaustivo:

- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie;
- società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti;
- istituti di vigilanza;
- partiti e movimenti politici;
- sindacati;
- caf e patronati;
- società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas);
- imprese di somministrazione di lavoro e ricerca del personale;
- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione;
- società di call center;
- società che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento.

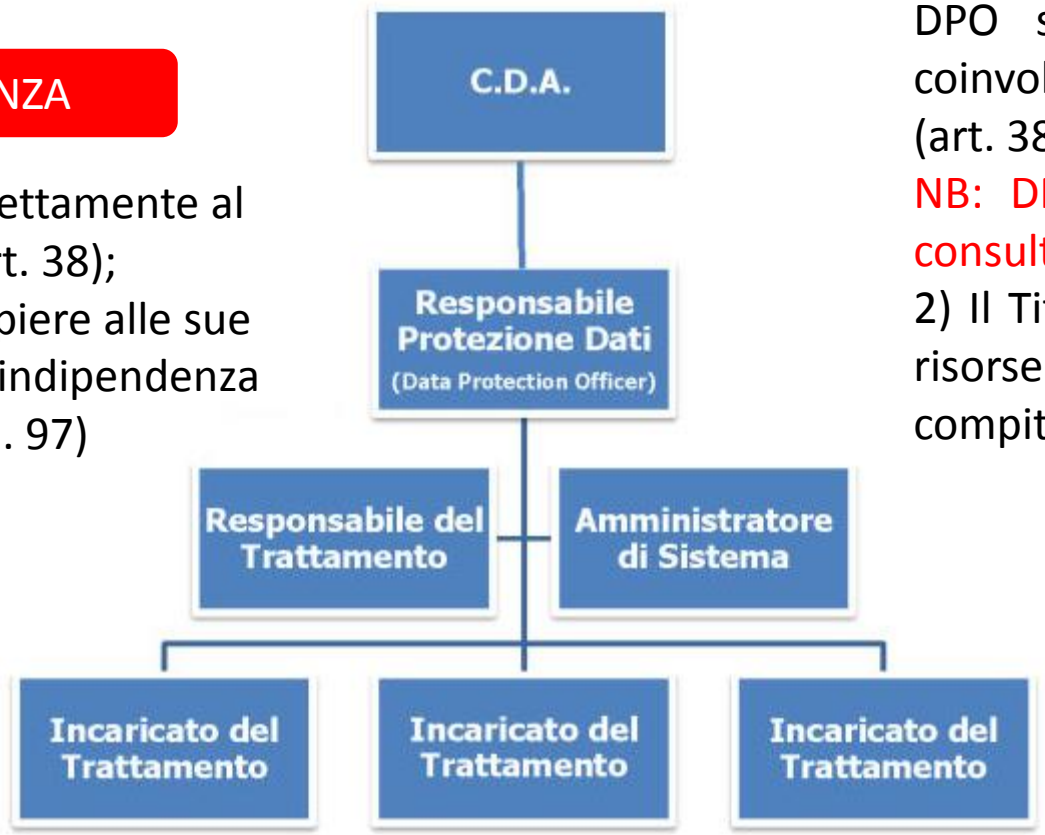
Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, Garante della Privacy, 29.03.2018

POSIZIONE DEL DPO

Art. 38

INDIPENDENZA

- Il DPO riferisce direttamente al vertice gerarchico (Art. 38);
- Il DPO deve adempiere alle sue funzioni in piena indipendenza (Vedi Considerando n. 97)

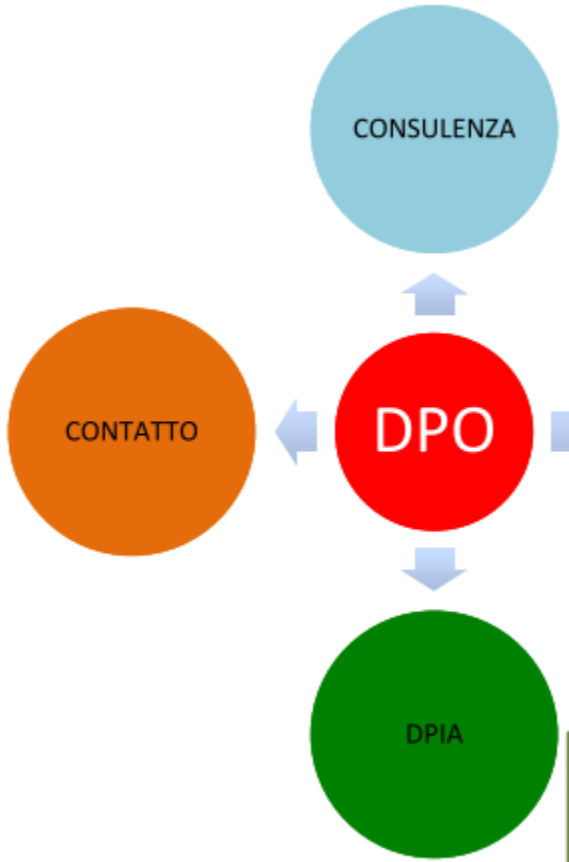


1) Il Titolare o Responsabile si assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni ad impatto privacy (art. 38).

NB: DPIA – L'art. 35 prevede che il DPO sia consultato nella Valutazioni di impatto privacy.

2) Il Titolare o il Responsabile devono fornire le risorse necessarie al DPO per svolgere i suoi compiti (art. 38)

COMPITI



- ✓ Coinvolto in questioni riguardanti la protezione dei dati (art. 38[1]);
- ✓ Informa e fornisce consulenza al Titolare, ai responsabili del trattamento nonché ai dipendenti (art. 39[1a]).

- ✓ Sorveglia l'osservanza della normativa in tema di protezione dei dati personali (art. 39[1b]);
- ✓ Vigila l'osservanza dei processi interni (art. 39[1b])

- ✓ Cooperare con l'Autorità Garante (art. 39[1d]);
- ✓ Fungere da punto di contatto con l'Autorità Garante (art. 39[1°])

Deve essere consultato dal Titolare nei casi di Valutazione di impatto privacy e rendere un parere (art. 35[2] e 39[1c])

GDPR: IL DECALOGO PER IL PROFESSIONISTA AL FINE DI TRATTARE I DATI PERSONALI IN CORRETTEZZA E SICUREZZA

dott. ing. Giuseppe Deleonibus

Il presente decalogo estrapola dagli adempimenti/obblighi in capo al titolare, sotto forma di quesiti, un nucleo essenziale di cautele/attenzioni che il professionista non deve mai dimenticare.
Con alcune avvertenze:
1) una normativa in materia di protezione dei dati personali è presente nell'ordinamento giuridico italiano dal 1996 e il cosiddetto 'GDPR' è portatore di indubbie novità ma non crea una disciplina dal nulla. Perciò il presente contributo non è effettivamente legato al solo GDPR e la necessità di aggiornamento rispetto alle sue disposizioni è l'occasione per tornare a valutare in generale l'organizzazione dello studio professionale sotto il profilo delle attività di trattamento;
2) il presente decalogo non ha e non può avere pretesa di esaustività. È uno spunto per un'autovalutazione che deve essere, nondimeno, completa e anche specifica, cioè tarata sulla concreta realtà dello studio professionale; realtà sotto il cui ombrello si possono annoverare tante diverse fattispecie, dal singolo professionista senza collaboratori allo studio associato con praticanti e personale dipendente;
3) l'interesse che ha il professionista a soddisfare i requisiti di integrità, disponibilità riservatezza e resilienza delle banche dati, precede l'esigenza di adempiere a norme di legge (al netto degli eccessi in esse presenti): è il corollario della concezione per la quale i dati personali sono costitutivi del patrimonio (immateriale) dell'organizzazione, come tali già meritevoli di protezione a prescindere da vincoli esterni.

	QUESITO	SPUNTO DI RIFLESSIONE
1	Ho predisposto la modulistica per procedere, durante il primo incontro con il Cliente, alla raccolta dei dati fornendo al medesimo una informativa completa, con un linguaggio semplice e chiaro?	La raccolta dei dati deve essere accompagnata – se non preceduta – da una informativa che contenga tutte le informazioni richieste dall'**art. 13** (oggi del **Testo Unico**, dal 25 maggio 2018 del **Regolamento**). Tra le novità del Reg.to figura il requisito del "linguaggio semplice e chiaro" dell'informativa.

	QUESITO	SPUNTO DI RIFLESSIONE
2	Ho organizzato le mie attività in modo da raccogliere e trattare solo ed esclusivamente i dati che mi sono necessari o utili in vista del miglior espletamento del mandato professionale ricevuto?	Il principio generale è presente tanto nel T.U. (**art. 11**) quanto nel Reg.to (**art. 5,** c.d. "minimizzazione dei dati"): si raccolgono e si trattano esclusivamente i dati personali che non siano "eccedenti" rispetto alle finalità del trattamento, ovvero che siano "limitati a quanto necessario rispetto alle finalità per le quali sono trattati". La disponibilità di dati estranei alla finalità esplicitata segnala la sussistenza di un trattamento 'abusivo', ulteriore e distinto.

	QUESITO	SPUNTO DI RIFLESSIONE
3	Ho organizzato la conservazione dei documenti relativi alle varie pratiche in modo da averne sempre, al momento giusto, la disponibilità ed in modo che i dati siano accessibili al solo personale autorizzato?	Qui si congiungono le esigenze generali della disponibilità e della riservatezza delle banche dati. La loro traduzione concreta è una gestione ordinata dei dati e delle informazioni – ovvero dei fascicoli cartacei e delle cartelle digitali - che ponga i rispettivi contenuti al riparo da sguardi indiscreti ovvero da accessi di estranei ma che allo stesso tempo consenta al titolare di gestire con efficienza le attività.

	QUESITO	SPUNTO DI RIFLESSIONE
4	Ho nominato e adeguatamente istruito i miei collaboratori ed altresì ho formalizzato i rapporti con i professionisti ai quali mi rivolgo per la gestione e lo sviluppo delle attività dello studio?	Tutto l'organigramma 'privacy' dello studio deve essere coinvolto nella politica di protezione dei dati. E' un organigramma ampio, in cui rientrano gli incaricati (collaboratori, praticanti, dipendenti) ma anche i responsabili dei trattamenti, cioè i professionisti esterni che a vario titolo collaborano con lo studio (avvocati di altri fori, commercialista, consulente del lavoro, ecc.). Osservando che: - per gli incaricati occorre una nomina (**art. 30 T.U.**) contenente peraltro le istruzioni operative per i trattamenti (di cui anche all'**art. 29 Reg.to**) - per i responsabili dei trattamenti, occorre un contratto (o altro atto giuridico) che vincoli i medesimi a specifici obblighi (**art. 28 Reg.to**).

	QUESITO	SPUNTO DI RIFLESSIONE
5	I miei pc sono protetti dalle minacce esterne? Dispongo, in caso di bisogno, del nominativo di un tecnico-informatico di fiducia al quale chiedere la soluzione di specifici problemi?	Il riferimento è all'implementazione di software adeguati a prevenire attacchi o minacce di vario genere e provenienza. In tal senso può essere saggio affidarsi alla competenza e all'esperienza di un professionista, rammentando che il Reg.to richiede misure “adeguate” rispetto alle caratteristiche, modalità e contesto dei trattamenti.

	QUESITO	SPUNTO DI RIFLESSIONE
6	Pc portatili e altri strumenti informatici rimovibili sono utilizzati nelle attività al di fuori dello studio in modo da minimizzare i rischi di perdita accidentale, sottrazione fraudolenta e similari?	L'esempio lampante è nell'uso della penna usb: premessa l'operatività di una valida password di accesso, è necessario caricare/lasciare nella penna esclusivamente i dati che debbano essere trattati nel corso della sessione esterna.

	QUESITO	SPUNTO DI RIFLESSIONE
7	Provvedo ad eseguire un salvataggio integrale (back up) di tutti i dati su pc perlomeno 1 volta alla settimana?	A parte la prescrizione di cui all'**Allegato B al T.U.**, questa operazione è davvero fondamentale per la protezione dei dati dello studio. In relazione alla intensità delle modifiche/inserimenti quotidiani, è prudente programmare una frequenza maggiore di quella minima.

	QUESITO	SPUNTO DI RIFLESSIONE
8	Ho definito un tempo di conservazione dei dati personali in linea con le finalità dei trattamenti?	Anche il professionista è tenuto, come ogni titolare, a definire il periodo di conservazione dei dati (che non possono essere conservati *ad libitum*) e, peraltro (novità del Reg.to), a farne oggetto di apposita menzione nell'informativa (in alternativa al periodo di conservazione sarà sufficiente indicare i criteri utilizzati per determinarlo).

	QUESITO	SPUNTO DI RIFLESSIONE
9	Quando devo rottamare pc, notebooks e altri strumenti elettronici utilizzati per le attività dello studio, mi assicuro che la dismissione avvenga nel rispetto della esigenza di protezione dei dati?	La c.d. 'spazzatura elettronica', quando non gestita, è malaugurata fonte di informazioni a tutto discapito degli interessati e con rischi per lo stesso titolare del trattamento. E' doveroso il rinvio a quanto stabilito dal Garante nel provvedimento del 5 dicembre 2008 (con le connesse istruzioni operative).

	QUESITO	SPUNTO DI RIFLESSIONE
10	Mi sono preoccupato della sicurezza fisica dello studio, nel senso di adottare misure o cautele atte ragionevolmente a prevenire accessi indesiderati e azioni concretantesi nella lesione della riservatezza, della disponibilità, della integrità delle banche dati?	E' sempre in evidenza il problema della sicurezza dei trattamenti. Stavolta, però, esso è valutato attraverso la disamina dei locali/luoghi fisici in cui si svolgono le attività dello studio. Le misure di protezione “adeguate”, anche qui, possono variare in ragione del contesto (ad es., studio localizzato in stanza all'interno di unità immobiliare dove sono presenti altri professionisti, studio localizzato al piano terra di un condominio, ecc.).

Riepilogando, COSA BISOGNA FARE?

1. Analizzare quali sono i dati di cui si dispone e fare una mappatura aggiornata dei dati;
2. Fare un inventario delle proprie informative e verificare come potrebbero cambiare in funzione delle nuove regole. Valutare cosa significa in concreto dover introdurre l'indicazione della fonte dei dati e il tempo di conservazione dei dati. Sperimentare nuove forme di informative visuali basate su icone;
3. Analizzare i processi di gestione delle istanze degli interessati e verificare come gestire questi processi avvalendosi di sistemi informatici e user friendly;
4. Dotarsi di "software sentinella" per gestire il nuovo obbligo di notifica delle violazioni nell'uso dei dati personali e verificare l'eventuale flusso extraeuropeo dei dati usando servizi cloud;
5. Sperimentare la Privacy by Design e effettuare il Privacy Impact Assessment affidandosi a esperti competenti che aiutino l'azienda a minimizzare gli impatti e a contenere i costi di gestione dei nuovi adempimenti. Pensare a come introdurre, eventualmente, un Data Protection Officer in azienda;
6. Analizzare gli effetti del diritto alla portabilità dei dati e adottare cautele organizzative per evitare impatti gravi sulla stabilità dei data base aziendali;
7. Definire le nuove regole di acquisizione e documentazione del consenso. Verificare con cura i fornitori dei dati. Questo è il tempo in cui fare test, test e ancora tet!
8. Verificare se trattate dati di minori e tenere conto che le nuove regole impongono di gestire anche il consenso degli esercenti la potestà dei genitori insieme al consenso del minore al di sotto dei 16 anni.

opera professioni

...e non finisce qui...

50 dei 99 articoli del Regolamento Europeo rimandano a norme attuative e norme nazionali di esecuzione.

Anche i Garanti nazionali emaneranno norme per anticipare l'entrata in vigore di alcuni aspetti del Regolamento e favorire l'armonizzazione tra i diversi ordinamenti.

Quindi nei prossimi mesi ci sarà molto da fare per adeguarsi alle nuove norme.

Per le aziende che trattano in modo significativo dati personali sarà importante definire un action plan e attivare un processo di adeguamento che segua costantemente le novità che si susseguiranno.

*La **data protection** sarà sempre di più un **fattore competitivo e favorirà le aziende che capiranno che** non **si tratta** più solo di una serie di adempimenti da gestire ma **di un processo organizzativo aziendale che ha natura produttiva e non solo normativa.***

Grazie per l'attenzione

dott. ing. Giuseppe Deleonibus
cell.: 3282612118 – 3896354758
mail: deleonibus@tecsial.it

Il presente documento è stato predisposto dal dott. ing. Giuseppe Deleonibus per la formazione e l'aggiornamento di liberi professionisti, consulenti, cittadini, studenti.