

# Tutto quesiti: gli adempimenti “privacy” per l’adeguamento al regolamento comunitario

Le risposte alle domande dei professionisti

di Armando Urbano | 11 MAGGIO 2018



Si prosegue nella disamina dei quesiti posti dai lettori in tema di *privacy*, con particolare riferimento alla situazione degli studi associati, degli studi professionali, delle s.r.l., delle società di servizi e del ruolo dei consulenti del lavoro. La casistica affronta i temi dell’individuazione dei dati sensibili, della tenuta del registro delle attività di trattamento, dell’informativa, dell’acquisizione del consenso, delle eventualità di *data breach*, della conservazione dei dati, nonché i profili sanzionatori.

## SOMMARIO:

- **QUESITO 1 - STUDIO ASSOCIATO**
- **QUESITO 2 - NOMINA DEL DPO NELLO STUDIO ASSOCIATO**
- **QUESITO 3 - DATI SENSIBILI**
- **QUESITO 4 - IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO**
- **QUESITO 5 - IL CONSENSO DELL’INTERESSATO**
- **QUESITO 6 - STUDIO PROFESSIONALE CON UN DIPENDENTE: OBBLIGO DEL REGISTRO DEI TRATTAMENTI**
- **QUESITO 7 - “DATA BREACH” DA PARTE DEL RESPONSABILE ESTERNO DEL TRATTAMENTO**
- **QUESITO 8 - INCARICHI DEL TITOLARE DI UNO STUDIO PROFESSIONALE**
- **QUESITO 9 - RESPONSABILE DEL TRATTAMENTO IN UNA SOCIETÀ DI SERVIZI**
- **QUESITO 10 - STUDIO ASSOCIATO DI RIDOTTE DIMENSIONI**
- **QUESITO 11 - FIGURE “PRIVACY” IN UNA SOCIETÀ A RESPONSABILITÀ LIMITATA**
- **QUESITO 12 - LICEITÀ DEL TRATTAMENTO**
- **QUESITO 13 - LA CONSULENZA DEL LAVORO E I DATI SENSIBILI**
- **QUESITO 14 - INFORMATIVA AI DIPENDENTI/FORNITORI/CLIENTI**
- **QUESITO 15 - INTEGRAZIONE INFORMATIVA EX ART. 13 DEL D.LGS. N. 196/2003**
- **QUESITO 16 - AUTONOMIA DEL DPO**
- **QUESITO 17 - ELABORAZIONE PAGHE DEI CLIENTI DI STUDIO DA PARTE DI CONSULENTE DEL LAVORO ESTERNO**
- **QUESITO 18 - DOCUMENTI CARTACEI**
- **QUESITO 19 - OBBLIGO DI SEGNALAZIONE DI “DATA BREACH”**
- **QUESITO 20 - CONSERVAZIONE DEI DATI**
- **QUESITO 21 - DIRITTO ALL’OBLIO**
- **QUESITO 22 - SANZIONI AMMINISTRATIVE**

## Quesito 1 – Studio associato

---

### *Domanda*

Un piccolo studio professionale associato (due persone in ambito familiare), con quattro dipendenti a tempo parziale, tratta dati sensibili. Facendo dichiarazioni dei redditi, quali sono gli obblighi minimi da rispettare?

### *Risposta*

Secondo quanto previsto dal GDPR, non vi sono più le misure minime da rispettare, in quanto ora si parla di **misure adeguate**.

In virtù del **principio di accountability (responsabilizzazione)**, ogni professionista deve adottare criteri e comportamenti tali da dimostrare la corretta adozione di misure finalizzate ad assicurare l'applicazione del regolamento in materia di protezione dei dati personali. Il titolare del trattamento effettua un processo di **valutazione** delle misure tecnico/organizzative che deve adottare per mitigare i rischi connessi al trattamento dei dati personali.

Poiché il Garante per la protezione dei dati personali ha precisato che non ritiene obbligatoria la **nomina del DPO "in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale"**, si ritiene che, **nel caso di studi associati**, tale nomina sia **obbligatoria**.

Il Consiglio nazionale dei dottori commercialisti ed esperti contabili ha elaborato, con la Fondazione nazionale commercialisti, una **check list di base per gli adempimenti privacy degli studi professionali** e la stessa è presente sul sito [www.commercialisti.it](http://www.commercialisti.it) (si veda la circolare monografica "[Privacy: check list di base per gli studi professionali](#)").

## Quesito 2 – Nomina del DPO nello studio associato

---

### *Domanda*

Uno studio professionale associato, in cui alcuni soci svolgono anche la funzione di revisore legale, è obbligato a nominare il DPO?

### *Risposta*

Sono **obbligati a nominare il DPO**, ai sensi dell'[art. 37](#), par. 1, lett. b) e c), del regolamento, tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala** o la cui attività principale consiste nel **trattamento, su larga scala, di dati sensibili**, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Il 26 marzo 2018, il Garante per la protezione dei dati personali ha chiarito che non ritiene obbligatoria la **nomina del DPO "in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale"**, mentre, non essendo stata espressamente esclusa, è **obbligatoria in presenza di studio associato**.

## Quesito 3 – Dati sensibili

---

### *Domanda*

Cosa si intende per dati sensibili? Nella pratica, uno studio professionale deve tenere il registro del trattamento?

In cosa consiste il registro del trattamento? Si deve tenere traccia di ogni accesso agli atti che si effettua durante il giorno e di chi fa accesso?

### *Risposta*

I dati sensibili sono quelli previsti dall'[art. 9](#) del Reg. (UE) 27 aprile 2016, n. 2016/679/UE, e sono rappresentati

dai **dati personali** che possono rivelare 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.

Il **registro delle operazioni di trattamento** deve essere tenuto da **tutti i titolari e i responsabili di trattamento, eccettuati** i titolari che trattano dati occasionalmente e gli organismi con meno di 250 dipendenti.

---

**⚠ Attenzione**

Se si trattano **dati sensibili**, la **tenuta del registro è obbligatoria**, a prescindere dal numero dei dipendenti.

---

**Non vi è obbligo di tenere traccia degli accessi** effettuati durante il giorno.

## Quesito 4 – Il registro delle attività di trattamento

---

### *Domanda*

Il registro dei trattamenti svolti è informatico? Con che dati si deve compilare?

### *Risposta*

Il registro delle attività di trattamento ha lo scopo di disporre un **quadro aggiornato dei trattamenti in essere** all'interno di un'azienda o di un soggetto pubblico ed è indispensabile per ogni valutazione e analisi del rischio.

Deve avere **forma scritta**, anche elettronica, e deve essere **esibito, su richiesta**, al Garante.

Esso **contiene**:

- i dati e il contatto del titolare del trattamento, del contitolare, del rappresentante e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;
- eventuali trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale;
- eventuali termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- la descrizione generale delle misure di sicurezza, tecniche e organizzative.

## Quesito 5 – Il consenso dell'interessato

---

### *Domanda*

I consensi acquisiti sui moduli fatti sottoscrivere nel tempo sulla base del [D.Lgs. 30 giugno 2003, n. 196](#), devono essere riacquisiti su nuovi moduli?

### *Risposta*

I **consensi** devono essere **nuovamente acquisiti** dagli interessati **sulla nuova informativa** che il professionista deve rendere al cliente.

## Quesito 6 – Studio professionale con un dipendente: obbligo del registro dei trattamenti

---

### Domanda

Nel caso di un professionista con un dipendente vige l'esonero dal registro trattamenti, in quanto i dipendenti sono meno di 250 oppure si è tenuti al registro trattamenti, perché trattasi di dati sensibili?

### Risposta

Il registro delle operazioni di trattamento deve essere tenuto da **tutti i titolari e i responsabili del trattamento dei dati**, fatta **eccezione** dei **titolari che trattano dati occasionalmente**. In deroga all'[art. 30](#), par. 5, del Reg. (UE) n. 2016/679/UE, si vedano la comunicazione WP 29 del 19 aprile 2018 e il Considerando 82 sulle finalità del registro.

## Quesito 7 – “Data breach” da parte del responsabile esterno del trattamento

---

### Domanda

Se il consulente del lavoro è un responsabile “esterno” del trattamento, in caso di *data breach*, causato da inadempimento nella tutela degli archivi del consulente del lavoro, ne risponde il titolare del trattamento? Eventualmente, poi, il cliente si potrà rivalere sul consulente del lavoro?

### Risposta

Il consulente del lavoro nominato responsabile del trattamento deve consegnare al titolare del trattamento un'**attestazione** nella quale comunica di essere **in regola con la normativa** in materia di protezione dei dati personali; in caso di **data breach sugli archivi del consulente del lavoro**, sarà quest'ultimo a dovere effettuare la **segnalazione al Garante** e, nei casi più gravi, dovrà segnalare l'evento anche all'interessato.

---

#### Attenzione

Qualora l'interessato dovesse riscontrare la mancata attuazione delle misure previste dal Reg. (UE) [n. 2016/679/UE](#) da parte del consulente del lavoro, potrà avviare l'azione per il **risarcimento del danno** nelle sedi competenti.

---

## Quesito 8 – Incarichi del titolare di uno studio professionale

---

### Domanda

Il titolare di uno studio professionale, con o senza dipendenti, può essere:

- titolare del trattamento;
- responsabile del trattamento;
- DPO?

Inoltre, può svolgere la valutazione iniziale in collaborazione con un tecnico informatico e successivamente effettuare l'aggiornamento in autonomia?

### Risposta

Nello studio professionale individuale, il **professionista è il titolare del trattamento**; il **responsabile del trattamento viene designato dal titolare**, al fine di tutelare i dati personali per suo conto.

Potrebbe esserci o meno il responsabile del trattamento esterno, ma, sicuramente, la figura non coincide con il titolare del trattamento.

Nello studio professionale individuale **non è obbligatorio nominare il DPO**.

La valutazione della **privacy by design** può essere effettuata con o senza collaborazione di un tecnico informatico; l'essenziale è che vengano adottati criteri e comportamenti tali da dimostrare la corretta adozione delle misure finalizzate ad assicurare l'applicazione del regolamento.

Si consiglia comunque di richiedere la collaborazione di figure idonee, che possano rilasciare un'**attestazione degli interventi effettuati**, per dimostrare, agli organi di controllo, di avere ottemperato a quanto richiesto dalla normativa.

## Quesito 9 – Responsabile del trattamento in una società di servizi

---

### *Domanda*

In una società di servizi con due soli soci la figura del responsabile del trattamento può essere omessa e, nel caso, il titolare del trattamento può assumere le responsabilità del responsabile del trattamento?

### *Risposta*

Nelle società il **titolare del trattamento è la società stessa** e le funzioni vengono assunte dal **legale rappresentante**. Qualora ve ne fosse bisogno, il **responsabile del trattamento**, soggetto esterno, viene **designato dal titolare**, qualora il trattamento dei dati sia effettuato da soggetti terzi.

## Quesito 10 – Studio associato di ridotte dimensioni

---

### *Domanda*

Per quanto riguarda gli studi associati di ridotte dimensioni, esistono ulteriori semplificazioni oltre all'esenzione dalla tenuta del registro dei trattamenti? Quali competenze a livello informatico deve avere la figura del DPO e quali sono le protezioni richieste a livello informatico per il trattamento dei dati da verificare?

### *Risposta*

Se lo studio associato, pur se di ridotte dimensioni, tratta i **dati sensibili** del cliente, deve obbligatoriamente **istituire il registro delle operazioni di trattamento**.

Il **responsabile della protezione dei dati** (DPO), nominato dal titolare del trattamento o dal responsabile del trattamento, **deve**:

1. possedere un'**adeguata conoscenza della normativa** e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a *master* e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;
2. adempiere alle sue funzioni in piena **indipendenza** e in **assenza di conflitti di interesse**. In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. operare alle **dipendenze del titolare o del responsabile** oppure sulla base di un **contratto di servizio** (RPD/DPO esterno).

Le **protezioni richieste a livello informatico** dovranno essere valutate, in maniera specifica, da un tecnico

informatico, o da un DPO, o da un'altra figura in possesso delle specifiche competenze; questo soggetto dovrà rilasciare una documentazione che attesti che la struttura ha adottato i mezzi idonei alla protezione da trattamenti non autorizzati od illeciti, dalla perdita, distruzione o dal danno accidentale (integrità dei dati).

## Quesito 11 – Figure “privacy” in una società a responsabilità limitata

---

### *Domanda*

Il quesito riguarda una società a responsabilità limitata, con un amministratore unico, in cui lo studio è “diviso” in tre professionisti commercialisti (uno dei quali è l'amministratore unico) che hanno anche una propria partita IVA individuale (che utilizzano solo per collegi sindacali e per procedure concorsuali) e che gestiscono i propri clienti facendo fatturare la società. I vari clienti hanno come riferimento esclusivo uno dei tre professionisti. La società utilizza anche ulteriori quattro professionisti (collaboratori) con la propria partita IVA, che sostanzialmente fatturano esclusivamente alla società. Visto che l'amministratore unico deve essere il titolare del trattamento, è possibile nominare più responsabili del trattamento (visto che la società è divisa in tre “settori” autonomi, che fanno capo ai tre professionisti)? Anche perché, indicando nell'informativa il titolare, un responsabile e il DPO, si rischierebbe di rilasciare un'informativa al cliente di uno dei tre professionisti (quello non titolare e non responsabile), senza che sia citato il suo nome. Ovviamente, i quattro professionisti (collaboratori) sarebbero tutti sub-responsabili relativi al professionista proprio di riferimento.

Per quanto riguarda i clienti propri a cui i singoli professionisti fatturano con la propria partita IVA, facendosi aiutare dai propri collaboratori, bisogna nominare un DPO?

### *Risposta*

Nel rispondere alla domanda, si ipotizza che i tre commercialisti siano tutti soci della società, perché tale situazione non è stata ben specificata.

Nella società a responsabilità limitata, il **titolare del trattamento è la società** e le relative scelte da assumere sono in capo al **legale rappresentante**.

Il titolare del trattamento può **nominare anche più responsabili del trattamento**, scegliendoli in base alle funzioni amministrative esercitate o alle aree territoriali in cui operano, oppure in base al ruolo svolto nel campo informatico.

Nel caso di società, dovrà essere **nominato anche il DPO**.

Il ruolo di responsabile della protezione dei dati personali (DPO) può essere ricoperto da un dipendente/collaboratore del titolare o del responsabile.

E' stato precisato che il ruolo di responsabile della protezione dei dati personali è **compatibile con altri incarichi**, a condizione che **non sia in conflitto di interessi** con essi.

Viene comunque consigliato di evitare l'assegnazione di tale ruolo a soggetti con incarichi di alta direzione (amministratore delegato, membro del consiglio di amministrazione, direttore generale, ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione *marketing*, ecc.).

L'**informativa** dovrà essere **resa dalla società** per i clienti (interessati) della stessa; mentre, per i **singoli clienti** dei professionisti, dotati di autonoma posizione fiscale, questi dovranno **singolarmente rendere l'informativa** ai propri clienti ed ottenere da questi il consenso espresso e, per loro, non sarà necessario nominare il DPO.

## Quesito 12 – Liceità del trattamento

---

### *Domanda*

L'**art. 6** prevede che il trattamento è lecito quando necessario per adempiere ad obblighi contrattuali. Quindi, un mandato professionale esonera da tutto?

### *Risposta*

L'[art. 6](#) tratta la liceità del trattamento e **non riguarda l'esonero dagli obblighi in materia di *privacy***.

Il mandato professionale legittima il trattamento dei dati, ma lo studio professionale deve ottemperare a tutte le prescrizioni in materia di *privacy* previste dal Reg. (UE) n. 2016/679/UE.

## Quesito 13 – La consulenza del lavoro e i dati sensibili

---

### *Domanda*

I dati per elaborare le paghe e i 730 sono considerati dati sensibili?

### *Risposta*

I dati trattati dallo studio del professionista, per elaborare le paghe e i modelli 730, **possono essere sensibili**, se, per esempio, sono conservati dati sulle spese mediche, sul credo religioso (scelta dell'8 per mille), trattenute del quinto dello stipendio o della pensione, pignoramenti da parte di terzi, assegni familiari, [legge n. 104/1992](#), cartelle cliniche contenenti le patologie, ecc.).

## Quesito 14 – Informativa ai dipendenti/fornitori/clienti

---

### *Domanda*

Con il nuovo GDPR bisogna rimpostare e consegnare la nuova informativa *privacy* ai dipendenti/fornitori/clienti?

### *Risposta*

Se l'informativa *privacy* in uso non rispetta quanto stabilito dagli [artt. 13](#) e [14](#) del Reg. (UE) n. 2016/679/UE, deve essere **nuovamente impostata** e consegnata ai vari soggetti, i quali dovranno esprimere il **consenso** al trattamento dei dati.

## Quesito 15 – Integrazione informativa ex [art. 13](#) del D.Lgs. n. 196/2003

---

### *Domanda*

Può mantenersi valida l'informativa basata sull'[art. 13](#) del D.Lgs. n. 196/2003, con le integrazioni previste dal nuovo regolamento comunitario?

### *Risposta*

L'informativa di cui all'[art. 13](#) del D.Lgs. n. 196/2003 **può essere integrata** con i contenuti previsti dagli [artt. 13](#) e [14](#) del Reg. (UE) n. 2016/679/UE.

## Quesito 16 – Autonomia del DPO

---

### Domanda

Come può essere DPO il "dipendente", se tale soggetto non può avere un conflitto di interesse? Se non può essere un socio, un dipendente è assoggettato al potere datoriale.

### Risposta

Il Garante per la protezione dei dati personali ha precisato che il **ruolo di responsabile della protezione dei dati personali è compatibile con altri incarichi**, a condizione che **non sia in conflitto di interessi** con essi.

Viene comunque consigliato di evitare l'assegnazione di tale ruolo a soggetti con incarichi di alta direzione (amministratore delegato, membro del consiglio di amministrazione, direttore generale, ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione *marketing*, ecc.).

---

#### Attenzione

La persona individuata quale DPO non deve rivestire un ruolo all'interno dell'organizzazione che gli consenta di determinare finalità e modalità del trattamento.

---

È opportuno precisare che il **DPO** è un *manager* della *privacy*, che **deve**:

- **informare e consigliare** sia il titolare che il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi relativi alla protezione dei dati;
- **verificare** che la normativa e le misure interne adottate dal titolare siano correttamente attuate ed applicate;
- fornire **pareri circa la valutazione di impatto** sulla protezione dei dati, sorvegliandone gli adempimenti;
- fungere da **collegamento** sia con il Garante della *privacy*, che con gli interessati.

## Quesito 17 – Elaborazione paghe dei clienti di studio da parte di consulente del lavoro esterno

---

### Domanda

Se il consulente del lavoro opera ed elabora le paghe del cliente sul *server* dello stesso deve comunque rilasciare la certificazione?

### Risposta

Il regolamento non parla di certificazioni che il responsabile del trattamento deve rilasciare al titolare. La lettera di nomina che il titolare del trattamento rilascia al responsabile del trattamento identifica e perfeziona le modalità e le responsabilità del rapporto che lega il titolare al responsabile. Il **titolare del trattamento può richiedere al responsabile del trattamento l'esibizione del registro delle attività del trattamento**, al fine di una più puntuale conformità al principio di responsabilizzazione.

A parere di chi scrive, al fine di dimostrare la conformità al principio di "*accountability*", è opportuno che ogni responsabile del trattamento fornisca, al titolare del trattamento, apposita **dichiarazione scritta circa l'adozione di misure di sicurezza** ritenute idonee a garantire l'integrità dei dati, il loro corretto trattamento e la loro corretta conservazione.

Nel caso in questione, il consulente del lavoro, responsabile esterno del trattamento, non deve rilasciare l'attestazione nella quale comunica di essere in regola con la normativa in materia di protezione dei dati personali, in quanto utilizza direttamente il *server* del titolare del trattamento, ma, deve avere il registro delle attività di trattamento da esibire al titolare del trattamento su sua richiesta.

Se il consulente del lavoro elabora le paghe dei clienti dello studio, il **professionista dovrà indicare il consulente del lavoro nella propria informativa**, da rendere ai clienti, quale responsabile del trattamento esterno, per l'elaborazione delle paghe.



## Quesito 18 – Documenti cartacei

---

### *Domanda*

Dato che i documenti cartacei sono soggetti a "trattamento", anche per questi va fatta la valutazione di impatto? Vanno messi tutti "sotto chiave"?

### *Risposta*

Anche i documenti cartacei che contengono i dati personali o dati sensibili sono soggetti agli adempimenti previsti dal Reg. (UE) [n. 2016/679/UE](#). Infatti, tutti i **mobili all'interno dei quali sono contenuti i dati personali dei clienti devono essere dotati di serratura** e il titolare di trattamento deve mettere in atto tutte le misure di sicurezza idonee ad evitare l'intrusione fisica all'interno della struttura da parte di soggetti non autorizzati.

## Quesito 19 – Obbligo di segnalazione di “data breach”

---

### *Domanda*

Le segnalazioni devono essere fatte solo se il danno si è perpetrato? Se, pure riscontrata l'intrusione, la cosa è "rientrata", cioè si è ripristinato il tutto senza danni, la segnalazione *data breach* va fatta comunque?

### *Risposta*

A partire dal 25 maggio 2018, tutti i titolari dovranno **notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore** e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Pertanto, la **notifica** all'autorità dell'avvenuta violazione non è obbligatoria, essendo **subordinata alla valutazione del rischio** per gli interessati, che spetta al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione **anche gli interessati**, sempre "senza ingiustificato ritardo".

## Quesito 20 – Conservazione dei dati

---

### *Domanda*

I dati dei clienti con rapporti ormai conclusi devono essere cancellati dal *server*? E' ammessa la necessità di tenerli per esigenze anche storiche? Il regolamento ammette di potere tenere i dati per esigenze statistiche o per recuperare i crediti?

### *Risposta*

La determinazione del periodo di conservazione dei dati deve avvenire nel rispetto del **principio di limitazione della conservazione dei dati**, di cui all'art. 5, par. 1, del GDPR, e non potrà estendersi ad un arco temporale superiore a quello strettamente necessario per il raggiungimento delle finalità per cui i dati sono trattati.

Il professionista deve **stabilire già nell'informativa** da rendere al cliente un **termine per la cancellazione dei dati**; vista la tipologia di trattamenti effettuati dallo studio del professionista, si ritiene condivisibile il criterio civilistico che individua in **dieci anni** il periodo di conservazione dei documenti rilevanti ai fini contabili, tributari e antiriciclaggio (in quest'ultimo caso, dieci anni dalla cessazione del rapporto con il cliente).



Nulla vieta di potere inserire anche un termine più lungo.

Si ritiene che **non sia possibile derogare** a quanto stabilito nell'informativa, anche se i dati vengono conservati per esigenze del professionista, anche di natura storica, statistica o per il recupero del credito.

## Quesito 21 – Diritto all'oblio

---

### Domanda

In cosa consiste il diritto all'oblio?

### Risposta

Rappresenta l'**interesse di un soggetto ad essere dimenticato**, mediante la **cancellazione dei contenuti**, dalle varie pagine *web*, di precedenti informazioni (spesso pregiudizievoli come, ad esempio, precedenti penali) che non rappresentano più la vera identità dell'interessato.

Vi è, dunque, la possibilità di richiedere l'eliminazione di notizie relative a fatti avvenuti in passato, per tutelare la riservatezza e l'identità personale attuale di un soggetto.

## Quesito 22 – Sanzioni amministrative

---

### Domanda

In caso di violazioni della normativa *privacy*, a quanto ammontano le sanzioni?

### Risposta

Fino a euro 10.000.000 (per le imprese, fino al 2 per cento del fatturato annuo, se superiore), **in caso di violazione dei seguenti obblighi:**

- misure di protezione *by-design, by-default*;
- nomina del rappresentante del titolare o dei responsabili non stabiliti nell'UE;
- accordo tra contitolari per le responsabilità;
- consenso dei minori in merito a servizi della società dell'informazione;
- tenuta del registro dei trattamenti;
- adozione di misure di sicurezza adeguate;
- comunicazione di *data breach*;
- DPIA;
- designazione del DPO.

Fino a euro 20.000.000 (per le imprese, fino al 4 per cento del fatturato annuo, se superiore), **in caso di violazione dei seguenti obblighi:**

- principi generali del trattamento dei dati;
- condizioni di liceità, per il consenso o per la revoca;
- norme trattamento di dati particolari, sensibili o giudiziari;
- mancato rispetto diritti dell'interessato;
- mancato rispetto principi per il trasferimento di dati extra-UE;
- norme nazionali in materia di rapporti di lavoro, archivi storici, ricerca scientifica.

## Riferimenti normativi:

- Reg. (UE) 27 aprile 2016, [n. 2016/679/UE](#);
- D.Lgs. 30 giugno 2003, n. 196, [art. 13](#).

### DOCUMENTI SUGGERITI



Tutto quesiti: le principali novità "privacy" per lo studio professionale  
**09 MAGGIO 2018**



"Privacy": check list di base per gli studi professionali  
**07 MAGGIO 2018**



"Privacy": il responsabile della sicurezza dei dati personali  
**11 APRILE 2018**

## Argomenti trattati

**PRIVACY**

**TRATTAMENTO DATI PERSONALI**

**TITOLARE DEL TRATTAMENTO DEI DATI**

**RESPONSABILE DEL TRATTAMENTO DEI DATI**

**RESPONSABILE DELLA PROTEZIONE DEI DATI**