FAQ PER GLI ORDINI DEGLI AVVOCATI
in materia di Protezione dei Dati Personali

Roma, il 28 marzo 2018

A decorrere dal 25 maggio 2018 troverà definitiva applicazione il Regolamento UE 2016/679, in materia di protezione dei dati personali, che introduce significative novità, di immediata applicazione per gli Enti Pubblici e, conseguentemente, anche per gli Ordini.

Le principali novità riguardano:
- l'introduzione del principio di responsabilizzazione (*accountability*);
- l'istituzione del registro dei trattamenti;
- la designazione di un Responsabile della Protezione dei Dati (RPD - *Data Protection Officer* - DPO)
- la notifica di eventuali *data breach*.

Ferma restando la possibilità di intervento del legislatore su aspetti del Regolamento che sono lasciati alla determinazione dei singoli Stati, la Commissione Privacy ha ritenuto di elaborare delle FAQ, per fornire ai COA delle prime indicazioni in merito agli adempimenti da adottare nell'immediato.

Il presente documento è soggetto ad integrazioni e modifiche, anche alla luce delle eventuali modifiche normative e future indicazioni e linee guida a livello nazionale ed europeo.
Roma, 28 marzo 2018

La Commissione Privacy

Cons. Avv. Carla Secchieri (Coordinatrice)
Avv. Nicola Fabiano (Componente esterno)
Avv. Giovanni Battista Gallus (Componente esterno)
Avv. Francesco Paolo Micozzi (Componente esterno)
Avv. Alessio Pellegrino (Segretario della Commissione)

1. IL REGOLAMENTO UE 2016/679 SI APPLICA AGLI ORDINI DEGLI AVVOCATI

Sì. Il "Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (Regolamento generale sulla protezione dei dati - RGPD, qui di seguito con il termine inglese GDPR) si applica a tutti i soggetti, pubblici e privati, stabiliti in Europa (artt. 2 e 3 del GDPR) e pertanto anche agli Ordini degli Avvocati (COA), quali Enti Pubblici non economici.

2. LA SCANSIONE TEMPORALE DEGLI ADEMPIMENTI PER L'ATTUAZIONE DEL REGOLAMENTO

Il Garante della protezione dei dati personali ha dato precise indicazioni agli Organismi pubblici indicando la centralità del principio di "responsabilizzazione" (cd. accountability), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali, e individuando le priorità fondamentali:

1. La designazione in tempi stretti del Responsabile della protezione dei dati (DPO);
2. L'istituzione del Registro delle attività di trattamento;
3. La notifica de(gli eventual)i *data breach* (e la introduzione di specifiche procedure da attivare a seguito delle eventuali violazioni).

Oltre alle priorità individuate dal Garante, appare importante attivarsi, prima del 25 maggio, per:

A. Aggiornare l'informativa, sulla base degli artt. 12 e ss del GDPR;
B. Riesaminare le politiche interne in tema di trattamento di dati personali, ai sensi dell'art. 24 del GDPR, provvedendo anche a definire in maniera adeguata i ruoli e assicurarsi che tutti coloro che trattano dati personali ricevano adeguate istruzioni e formazione (ex art. 29 del GDPR);
C. Procedere alla verifica dei sistemi informatici, per assicurare il rispetto dei principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita di cui all'art. 25 GDPR (concetti di privacy-by-default e privacy-by-design);
D. Esaminare i rapporti contrattuali con i responsabili esterni del trattamento, per verificarne la conformità (art. 28 del GDPR);
E. Verificare l'adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del GDPR;
F. Valutare se si debba procedere, per uno o più trattamenti, ad effettuare una valutazione d'impatto privacy (art. 35 del GDPR).

Tutti questi adempimenti presuppongono, peraltro, che ciascun Consiglio dell'Ordine e CDD abbia proceduto ad un'accurata ricognizione dei trattamenti di dati personali che

effettua nell'ambito delle proprie funzioni istituzionali, e dei rischi che su di essi incombono.

3. L'ORDINE DEGLI AVVOCATI DEVE RENDERE L'INFORMATIVA ?

I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. Si reputa, pertanto opportuno che l'Ordine renda l'informativa sia in applicazione del D.Lgs. 196/2003, sia in virtù di quanto stabilito dagli articoli 13 e 14 del GDPR.
Si ritiene sufficiente la pubblicazione dell'informativa sul sito web.
Non è, comunque, necessario fornire l'informativa:
a) se l'interessato dispone già dell'informazione;
b) se la registrazione o la comunicazione dei dati personali sono previste per legge (come, ad esempio i dati degli Albi, elenchi e registri ex art. 15 L 247/2012 e D.M. Giustizia 16 agosto 2016 n.178) ;
c) se informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato.

- All. A: schema di informativa

4. L'ORDINE DEGLI AVVOCATI DEVE TENERE UN REGISTRO DEI TRATTAMENTI ?

Sì. Ai sensi dell'articolo 30 del GDPR "*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità*".
Il Registro dei Trattamenti (elettronico o cartaceo) è uno strumento fondamentale non soltanto allo scopo di disporre di un quadro aggiornato ed accurato dei trattamenti svolti ed in essere all'interno Consiglio per la corretta valutazione ed analisi del rischio, ma anche ai fini dell'eventuale supervisione e richiesta di esibizione da parte del Garante. La tenuta del registro dei trattamenti non costituisce, infatti, un mero adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali.
Ancorché l'art. 30, sia pure con formulazione non troppo chiara, preveda ipotesi di esenzione dalla tenuta del registro, si tratta di un incombente imprescindibile, anche ai fini del principio di "responsabilizzazione", che impone al titolare non solo l'onere di rispettare i principi fondamentali in tema di trattamento di dati personali, ma anche di comprovarlo.

- Allegato B: schema di registro dei trattamenti

5. QUALI DATI PERSONALI TRATTANO ?

Appare superfluo ricordare che la definizione di dato personale contemplata dal GDPR è sulla medesima linea dell'attuale definizione prevista dal D.Lgs. 196/03. Dato personale è, pertanto, "qualsiasi informazione riguardante una persona fisica identificata o identificabile". La persona fisica, ai sensi del GDPR, si considera identificabile quando "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".

A titolo indicativo e non esaustivo, i COA sono titolari (determinano le finalità e/o i mezzi del trattamento) di dati personali:

- degli iscritti (dati personali e categorie particolari di dati come dati relativi alla salute art. 9 GDPR) ;
- dei consulenti del COA;
- dei dipendenti del COA;
- relativi ad atti amministrativi e fiscali;
- dei fornitori (persone fisiche);
- relativi agli esposti o alle denunce, o all'acquisizione di notizie di fatti suscettibili di valutazione disciplinare, dei quali cura la successiva trasmissione al CDD competente;
- relativi alle richieste di ammissione al patrocinio a spese dello Stato [art. 9 GDPR];
- di utenti relativi all'attività di Sportello al cittadino;
- relativi ai poteri di vigilanza, controllo e monitoraggio regolare e sistematico degli iscritti negli albi elenchi e registri ex art. 29 L 247/2012;
- inerenti l'acquisizione di segnalazioni circostanziate e puntuali sulla magistratura per il buon andamento dell'amministrazione della giustizia ed in riferimento ai compiti espressamente previsti *ex lege*, come i pareri ai Consigli Giudiziari.

6. L'ORDINE DEGLI AVVOCATI PUÒ NOMINARE DEI RESPONSABILI ESTERNI DEL TRATTAMENTO? CON QUALI FORMALITÀ?

Il Responsabile del trattamento ("Data Processor" nella versione anglofona) è definito dal GDPR come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento". Esempi tipici sono costituiti dai soggetti esterni incaricato della gestione del sito web, della posta elettronica o dei servizi cloud.

Tali soggetti, già nella sistematica del Codice della Privacy, devono essere nominati quali "responsabili".

L'art. 28 del GDPR delinea in dettaglio i rapporti tra titolare (Data Controller) e responsabile (Data Processor), stabilendo innanzitutto che si debba ricorrere a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

Se, infatti, un Responsabile del trattamento viola il GDPR non adempiendo agli obblighi normativi o agendo difformemente alle istruzioni impartite dal Titolare è considerato egli stesso Titolare del trattamento in questione e risponderà direttamente (o, se in corresponsabilità, in solido) per il risarcimento del danno cagionato all'interessato (ex art. 82), e delle sanzioni di cui agli artt.83 ed 84 del GDPR.

Perché i compiti, gli oneri ed i poteri nell'esecuzione dei trattamenti del Responsabile siano sempre chiaramente definiti, l'entità dei trattamenti dovrebbe essere specificatamente disciplinata da un contratto -individuando innanzitutto la materia disciplinata, 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, e comprenda tutti gli ulteriori elementi specificati nell'art. 28, comma 3, del GDPR- ovvero da un atto giuridico o da una norma cogente che vincoli il Responsabile del trattamento al Titolare del trattamento. È possibile scegliere un contratto individuale o clausole contrattuali tipo eventualmente adottate direttamente dalla Commissione oppure da un'Autorità (come il nostro Garante per la protezione dei dati personali).

Occorre poi disciplinare espressamente se il responsabile possa avvalersi o meno di sub-responsabili per il trattamento.

E' quindi importante che ogni COA provveda:

1. Alla verifica di eventuali contratti eventualmente già in essere, per accertarne la compatibilità con l'art. 28 del GDPR;
2. All'inserimento puntuale, nei bandi e contratti, delle pattuizioni necessarie per soddisfare i requisiti previsti dall'art. 28, anche con riguardo alle garanzie di rispetto dei principi del GDPR, che i responsabili devono possedere.

Questi adempimenti saranno facilitati, in futuro, dall'emanazione, da parte della Commissione europea o del Garante, di clausole contrattuali tipo.

7. L'ORDINE DEGLI AVVOCATI DEVE FARE UNA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)?

L'art. 35, par. 1, stabilisce che *"quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".* Il successivo par. 3, lettere a) e b) prevede che la valutazione d'impatto è richiesta nei casi:

a. *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 suddette persone fisiche;*

b. *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10".*

La valutazione d'impatto potrebbe rendersi quindi necessaria soprattutto per quei trattamenti su larga scale che comprendano dati sensibili e giudiziari. Uno degli esempi più rilevanti può essere costituito, anche in considerazione dell'elevato numero di domande ricevute dai COA, dai trattamenti effettuati per finalità di ammissione al beneficio del patrocinio a spese dello Stato. Anche in questo caso, quand'anche, in via meramente ipotetica, si potesse ritenere questo trattamento escluso dall'obbligo di DPIA, la peculiare natura dei dati trattati indurrebbe comunque, nell'ottica della responsabilizzazione, all'effettuazione della valutazione d'impatto (DPIA).

Al fine di agevolare il compito per gli obbligati, inseriamo qui di seguito il link al software, libero e gratuito, e disponibile per differenti piattaforme, che semplifica la predisposizione di una DPIA, e pubblicato sul sito web del CNIL (il Garante francese della Protezione dei Dati),.

Link al software per la DPIA: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

8. L'ORDINE DEGLI AVVOCATI DEVE DESIGNARE UN DPO ?

Sì. L'art. 37, par. 1, del GDPR recita testualmente che "*Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della*

protezione dei dati ogniqualvolta [...] *il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico* […]". In considerazione della natura di ente pubblico dell'Ordine degli Avvocati, esso sarà obbligato a nominare un Responsabile della Protezione dei Dati (o Data Protection Officer - DPO).

9. QUALI REQUISITI DEVE AVERE IL DPO?

Il paragrafo 5 dell'allegato A alle "Linee guida sui responsabili della protezione dei dati adottate il 13 dicembre 2016 [Versione emendata e adottata in data 5 aprile 2017]" in esplicazione dell'articolo 37, paragrafo 5 GDPR, chiarisce che il DPO "*è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i* [rispettivi] *compiti* [...] il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il DPO avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Fra le competenze e conoscenze specialistiche pertinenti rientrano le seguenti:

- adeguata conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati (compresa un'approfondita conoscenza del GDPR)[1];
- familiarità con le operazioni di trattamento svolte;
- familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile;
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile."

Il Garante della protezione dei dati personali, con newsletter n. 432 del 15 settembre 2017 (link), ha offerto le prime indicazioni su come scegliere il Responsabile della protezione dei dati personali (DPO): non facendo meramente riferimento ad attestazioni formali sul possesso delle conoscenze o l'iscrizione ad appositi albi professionali, ma verificando con particolare attenzione la presenza di competenze ed esperienze specifiche.
I DPO per i COA dovranno, infatti, avere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore ordinistico di riferimento. Nella selezione del DPO sarà opportuno in primo luogo privilegiare soggetti che possano dimostrare qualità

1 In chiarimento delle norme del GDPR anche il Garante italiano ha più volte ribadito che 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.

professionali adeguate alla complessità del compito da svolgere, che possano documentare le esperienze pregresse e la cui formazione sia adeguata (ad esempio con la partecipazione a master e corsi di studio/professionali, in particolare se risulta documentato il livello raggiunto, e se gli attestati ricevuti siano stati rilasciati all'esito di verifiche al termine di un ciclo). In riferimento alla formazione, il Garante, nella risposta a quesito del 28 luglio2017 (Doc-Web: 7057222) chiarisce che "gli schemi di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori […] rilasciate anche all'esito della partecipazione ad attività formative e alla verifica dell'apprendimento, possono rappresentare, al pari di altri titoli, uno strumento per valutare il possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del RPD (ndr. DPO)".
La normativa attuale non prevede l'obbligo per i candidati di possedere attestati formali delle competenze professionali come le certificazioni UNI, EN, ISO (le quali certificazioni, ribadisce nella stessa risposta, non sono rientranti tra quelle disciplinate dall'art. 42 del GDPR); Tali certificazioni volontarie, attestati di Corsi di studio/professionali, infatti, non possono sostituire in toto la valutazione e l'analisi del possesso dei requisiti del DPO necessari per svolgere i compiti da assegnargli in conformità all'art. 39 del GDPR, benché possano comunque essere elementi valutativi del possesso di un livello adeguato di conoscenza della disciplina. Elementi che devono essere considerati nell'insieme e legati indissolubilmente ad una valutazione dell'esperienza professionale, fattuale ed empirica, ovvero una valutazione autonoma del possesso dei requisiti necessari per svolgere i compiti assegnati al DPO.

10. QUALI SONO I COMPITI DEL DPO?

Il Responsabile della protezione dei dati dovrà, in particolare:

- **a.** sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- **b.** collaborare con il Titolare/Responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- **c.** informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- **d.** cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
- **e.** supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento .

11. PUÒ ESSERE DESIGNATO UN DPO INTERNO? E IN CHE CASO?

Sì."*Il responsabile della protezione dei dati può essere un dipendente del Titolare del trattamento o del Responsabile del trattamento*"(art. 37, par. 6, del GDPR) ed è designato in funzione delle qualità professionali, in particolare, come già visto, della (art. 37, par. 5):

- *conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati..."* determinata in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento*, e*
- *della capacità di assolvere i compiti di cui all'articolo 39*". Ciò significa, come chiarito nelle Linee guida, che "*il DPO, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati*".

Al dipendente deve essere assicurata l'assoluta autonomia ed indipendenza dal Titolare del trattamento (considerando 97). Nel GDPR vi sono numerose garanzie a presidio di questo principio:

- Il titolare o il responsabile del trattamento non possono impartire alcuna istruzione per quanto riguarda lo svolgimento dei compiti affidati al DPO (articolo 38, paragrafo 3);
- Il DPO non può essere penalizzato o rimosso dall'incarico in rapporto allo svolgimento dei propri compiti;
- Non deve sussistere alcuna ipotesi di conflitto di interessi, anche con riguardo a eventuali ulteriori compiti e funzioni.

Ciò significa, in primo luogo, che il DPO non può rivestire, all'interno dell'Ordine degli Avvocati (organizzazione del titolare del trattamento o del responsabile del trattamento), un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento.
Occorre altresì sottolineare che il Gruppo di lavoro Articolo 29 ha ritenuto che possa sussistere conflitto di interesse del DPO con i ruoli di amministratore delegato, di responsabile del personale e di responsabile del sistema informativo; ruoli normalmente ricoperti in ambito Ordinistico da dirigenti e funzionari che dovranno, pertanto, essere esclusi dalla selezione.

12. PUÒ ESSERE DESIGNATO UN UNICO DPO PER PIÙ ORDINI?

Ai sensi dell' articolo 37, paragrafo 3, è ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. L'articolo 37, paragrafo 2, consente di nominare un unico RPD a condizione che quest'ultimo sia "*facilmente raggiungibile da ciascuno stabilimento*".
Il concetto di raggiungibilità si riferisce ai compiti del DPO in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente, visto che uno dei compiti del DPO consiste nell'"i*nformare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento*".
Poiché il DPO è chiamato a una molteplicità di funzioni, il titolare del trattamento o il responsabile del trattamento deve assicurarsi che un unico DPO, se necessario supportato da un team di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.
Se l'unicità della figura del DPO è una condizione possibile, appare comunque opportuno procedere all'individuazione di più figure di supporto, con riferimento ai singoli Consigli dell'Ordine o a "settori" dell'Ordine (Consigli Distrettuali di Disciplina, Camere arbitrali, Organismi di mediazione e conciliazione, etc.) che facciano però riferimento a un unico soggetto responsabile, sia che la scelta ricada su un DPO interno (ad uno dei COA), sia che questa ricada su un DPO esterno.

13. IL DPO DEVE ESSERE NECESSARIAMENTE UNA PERSONA FISICA?

La funzione di DPO può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna. In tale ultimo caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale DPO soddisfi tutti i requisiti applicabili come fissati nella Sezione 4 del GDPR; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi. Pari importanza riveste il fatto che ciascuno dei soggetti in questione goda delle tutele previste dal GDPR: per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto DPO, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di DPO. Al contempo, si potranno associare le competenze e le capacità individuali affinché il contributo collettivo fornito da più soggetti consenta di rendere alla clientela un servizio più efficiente.
Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il team DPO, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del team DPO e di prevedere che sia un solo soggetto a

fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.
[Linee guida sui responsabili della protezione dei dati Adottate il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017)**]**

14. SE L'ORDINE HA UN SOLO DIPENDENTE O COMUNQUE NON HA FIGURE DIRIGENZIALI DEVE NOMINARE UN DPO ESTERNO?

Il DPO "*riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento*" (art. 38, par. 3, del GDPR). Tale rapporto diretto garantisce, in particolare, che il vertice amministrativo venga a conoscenza delle indicazioni e delle raccomandazioni fornite dal DPO nell'esercizio delle funzioni di informazione e consulenza a favore del titolare o del responsabile.
Alla luce delle considerazioni di cui sopra, nel caso in cui si opti per un DPO interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in contatto diretto con il vertice dell'organizzazione.
Quest'ultimo, affinché sia rispettata l'assenza di conflitto di interessi, occorrerà che non svolga comunque ulteriori funzioni assegnate che, come indicato nelle Linee guida, e come già approfondito al punto 10, possano comportare la definizione di finalità e modalità del trattamento dei dati.

In caso di nomina di un DPO interno, l'art 38 comma 5 GDPR chiarisce che "Il responsabile della protezione dei dati può svolgere altri compiti e funzioni". Le linee Guida, al par. 3.3, aggiungono che "*ciò significa che il RPD (DPO), nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare ad una specifica questione attinente alla normativa in materia di protezione dei dati*",

L' articolo 38, paragrafo 2 , del GDPR obbliga il titolare del trattamento o il responsabile del trattamento a sostenere il DPO "*fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*". Ciò si traduce, in modo particolare, nel poter disporre di tempo sufficiente per l'espletamento dei compiti affidati al DPO e questo presupposto riveste particolare importanza se viene designato un dipendente interno con un contratto part-time, oppure se lo stesso soggetto si occupi di protezione dati oltre a svolgere altre

incombenze. In caso contrario, il rischio è che le attività cui il DPO è chiamato finiscano per essere trascurate a causa di conflitti con altre priorità (Linee guida par. 3.2).
Per i motivi appena esposti, ancorché la nomina possa essere oggetto di valutazione caso per caso, si reputa sconsigliabile la nomina di un DPO interno qualora sia l'unico dipendente del Consiglio o, comunque, quando le figure professionali interne all'Ordine non soddisfino i requisiti essenziali e necessari previsti dal Regolamento. Ed in riferimento ai medesimi presupposti si reputa sconsigliabile la nomina di un DPO interno che non possa garantire le caratteristiche precipue di competenza, professionalità, autonomia ed indipendenza che deve (dimostrare di) possedere (quale requisito per la nomina stessa) il DPO.
Certamente in questo caso sarà possibile, per più ordini contigui, nominare un unico DPO.

15. PUÒ ESSERE NOMINATO DPO UN AVVOCATO ISCRITTO ALL'ORDINE ?

L'art 38 comma 5 GDPR chiarisce che "*Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi*". Astrattamente i doveri di segretezza e riservatezza del Responsabile della protezione dei dati in merito all'adempimento dei propri compiti sono tipici della professione forense (art. 13 CDF), così come il dovere di correttezza, di diligenza, competenza e preparazione professionale (artt. 12, 14, 15 CDF). In tal senso non appaiono delinearsi preclusioni e la qualifica di DPO ben può essere attribuita con un contratto di servizi ad un avvocato, il quale ha per peculiarità proprie della professione forense caratteristiche del Responsabile della protezione dei dati.
Ciononostante il complesso dei compiti assegnati al DPO aventi rilevanza sia interna (consulenza, pareri, sorveglianza sul rispetto delle disposizioni) sia esterna (cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti) sono impegnativi sia in termini di dedizione temporale sia in termini di diligenza intellettiva. Pertanto ogni singolo Consiglio dell'Ordine dovrà valutare caso per caso, sia considerando l'impegno base relativo al carico lavorativo tipico della figura, sia valutando le attività generali e peculiari del Consiglio (ad esempio in riferimento al numero di iscritti, se vi sono attivi Organismi interni per la mediaconciliazione, o per la risoluzione da crisi da sovraindebitamento, o per la risoluzione alternativa delle controversie; se è attivo e con che numeri di avventori lo Sportello al cittadino; se sono rilevanti le statistiche relative alle richieste di patrocinio a spese dello Stato etc.) se questa attività di Responsabile della protezione sia (o meno) compatibile con l'attività ordinaria e quotidiana, con il numero di cause e con gli impegni derivanti dalla professione forense del singolo avvocato.
Sarà, inoltre, senz'altro opportuno che il soggetto incaricato versi in una situazione di totale indipendenza rispetto al Consiglio dell'ordine stesso, inteso come Titolare del Trattamento.

16. UN CONSIGLIERE DELL'ORDINE PUÒ ESSERE NOMINATO DPO ?

Si ritiene che possa sussistere conflitto di interessi tra Consiglio e membro dell'Ordine dal momento che il Consigliere fa parte dell'organismo che è, nel contempo, Titolare del trattamento dati.

17. PER LA RICERCA DI UN DPO OCCORRE UN BANDO DI GARA ?

Stante la natura giuridica di enti pubblici non economici, gli Ordini professionali ricadono nell'ambito di applicazione del d.lgs. n. 50/2016, ai fini dell'affidamento dei contratti pubblici di servizi.
L'affidamento dell'incarico di DPO ben potrà seguire le procedure semplificate di cui all'articolo 36 del Codice dei contratti pubblici, ivi compreso l'affidamento diretto, nel rispetto dei principi di economicità, efficacia, tempestività, correttezza, libera concorrenza, non discriminazione, trasparenza, proporzionalità, pubblicità, rotazione degli inviti e degli affidamenti, nonché del principio di prevenzione e risoluzione dei conflitti di interessi.

18. QUALI SONO LE FORMALITÀ DI NOMINA DEL DPO?

Il GDPR prevede all'art. 37, par. 1, che il titolare e il responsabile del trattamento designino il RPD; da ciò deriva, quindi, che l'atto di designazione è parte costitutiva dell'adempimento. Nel caso in cui la scelta del RPD ricada su una professionalità interna all'ente, occorre formalizzare un apposito atto di designazione a "Responsabile per la protezione dei dati". In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto di servizi redatto in base a quanto previsto dall'art. 37 del RGP (per agevolare gli enti, in allegato alle Faq, è riportato uno schema di atto di designazione).
Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario (in conformità a quanto previsto dal quadro normativo di riferimento) che nello stesso:

- sia individuato in maniera inequivocabile il soggetto che opererà come RPD, riportandone espressamente
  - le generalità,
  - i compiti (eventualmente anche ulteriori a quelli previsti dall'art. 39 del GDPR),
  - le funzioni che questi sarà chiamato a svolgere in ausilio al titolare/responsabile del trattamento,
  - e l'eventuale assegnazione di compiti aggiuntivi.

L'eventuale assegnazione di compiti aggiuntivi rispetto a quelli originariamente previsti nell'atto di designazione, dovrà comportare la modifica e/o l'integrazione dello stesso o delle clausole contrattuali.
Nell'atto di designazione o nel contratto di servizi devono risultare succintamente indicate anche le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio RPD, al fine di consentire la verifica del rispetto dei requisiti previsti dall'art. 37, par. 5 del RGPD, anche mediante rinvio agli esiti delle procedure di selezione interna o esterna effettuata.
La specificazione dei criteri utilizzati nella valutazione compiuta dall'ente nella scelta di tale figura, oltre a essere indice di trasparenza e di buona amministrazione, costituisce anche elemento di valutazione del rispetto del principio di «responsabilizzazione». Una volta individuato, il titolare o il responsabile del trattamento è tenuto a indicare, nell'informativa fornita agli interessati, i dati di contatto del RPD pubblicando gli stessi anche sui siti web e a comunicarli al Garante (art. 37, par. 7).
Per quanto attiene al sito web, può risultare opportuno inserire i riferimenti del DPO nella sezione "amministrazione trasparente", oltre che nella sezione "privacy" eventualmente già presente. Come chiarito nelle Linee guida, in base all'art. 37, par. 7, non è necessario - anche se potrebbe costituire una buona prassi, in ambito pubblico - pubblicare anche il nominativo del DPO, mentre occorre che sia comunicato al Garante per agevolare i contatti con l'Autorità (anche in questo caso, in allegato alle Faq, è riportato un modello di comunicazione al Garante). Resta invece fermo l'obbligo di comunicare il nominativo agli interessati in caso di violazione dei dati personali (art. 33, par. 3, lett. b)

[Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD)] (Modello del Garante e/o bozza di modello) allegato:
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322273

19. C'È UN TERMINE PER LA NOMINA DEL DPO ?

Il GDPR sarà applicabile dal 25 maggio 2018. A tale data ciascun Ordine degli Avvocati dovrà aver nominato il proprio RPD/DPO.

20. E' ANCORA VALIDA L'AUTORIZZAZIONE GENERALE DATA DAL GARANTE[2]?

L'autorizzazione n. 4/2016 - Autorizzazione al trattamento dei dati sensibili da parte dei liberi professionisti - ha validità temporale sino al 24/5/2018. Il GDPR pone con forza

2 http://www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurarne l'applicazione (si vedano gli artt. 23-25, in particolare, e l'intero Capo IV del GDPR). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai Titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento stesso.
Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by default and by design*" (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "*al fine di soddisfare i requisiti*" del GDPR e tutelare i diritti degli Interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.
Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal Titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.

21. CHI È IL TITOLARE DEL TRATTAMENTO DEI DATI ?

Ai sensi dell'art. 4 comma 7 del GDPR Il titolare del trattamento è *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".*
Per quanto riguarda l'Ordine degli Avvocati, il Titolare del trattamento è il Consiglio, in persona del Presidente pro tempore

22. CI SONO SANZIONI PER IL MANCATO ADEGUAMENTO O PER LA MANCATA NOMINA DEL DPO ?

Ai sensi dell'articolo 58, par. 2 (lettere da a) a h) e j)) del GDPR l'Autorità di controllo, il Garante per la protezione dei dati, ha poteri di avvertimento, di ammonimento, di ingiunzione, di revoca della certificazione e di ordinare l'imposizione la rettifica, la

cancellazione di dati personali, la limitazione del trattamento o la sospensione dei flussi di dati. In aggiunta alle misure succitate, o in luogo di tali misure, l'Autorità - in funzione delle circostanze di ogni singolo caso - ha il potere di infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, par. 4 lett. a) fino a 10.000.000,00 di euro, fissando l'ammontare della stessa in ogni singolo caso tenendo debito conto degli elementi valutativi elencati nel medesimo articolo.
In riferimento alla responsabilità da illecito amministrativo occorre innanzitutto precisare che il GDPR è imperniato su una figura unica di responsabile per il danno cagionato dal suo trattamento, e questi è il Titolare del trattamento. I Responsabili del trattamento rispondono, infatti, per il danno causato dal trattamento solo se non hanno adempiuto agli obblighi del GDPR specificatamente loro diretti o se hanno agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento; ed il DPO non ha responsabilità dirette. E' senza dubbio ipotizzabile sul piano risarcitorio un diritto di rivalsa a favore del Titolare e del Responsabile cha abbiano subito un danno per colpa grave o inadempienze gravi riferibili ai compiti previsti per il DPO; purtuttavia quest'ultimo potere/diritto di rivalsa per responsabilità indiretta deve essere necessariamente temperato dalla responsabilità (diretta) dello stesso Titolare (o Responsabile) nello scegliere (avendo effettuato tutte le valutazioni previste dal GDPR) il DPO.

23. MISURE DI SICUREZZA[3]

Le misure di sicurezza devono "*garantire un livello di sicurezza adeguato al rischio"* del trattamento; in questo senso, la lista di cui al paragrafo 1 dell'art. 32 del GDPR è una lista c.d. aperta e non esaustiva (cfr. "*tra le altre, se del caso*"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 del D.Lgs 196/2003) poiché tale valutazione sarà rimessa, caso per caso, al Titolare e al Responsabile in rapporto ai rischi specificamente individuati come da art. 32 del GDPR.
Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.
Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità Garante per la protezione dei dati personali potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del GDPR) potranno restare in vigore (in base all'art. 6, paragrafo 2, del GDPR) le misure di sicurezza attualmente previste per i trattamenti di dati sensibili svolti dai Consigli dell'Ordine (e dai CDD) per finalità di rilevante interesse pubblico nel rispetto degli specifici

3 http://www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

regolamenti attuativi (ex artt. 20 e 22 D.Lgs. 196/2003[4]) laddove contengano disposizioni in materia di sicurezza dei trattamenti.

24. DATA BREACH (*Notifica delle violazioni di dati personali [5]*)

A partire dal 25 maggio 2018, tutti i Titolari - e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi - dovranno notificare all'autorità di controllo le violazioni di dati personali[6] di cui vengano a conoscenza, entro 72 ore dalla conoscenza e comunque "senza ingiustificato ritardo", a meno che sia improbabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati[7]. Pertanto, la notifica all'autorità dell'avvenuta violazione all'Autorità Garante sarà la regola, salva la valutazione, che spetta ancora una volta al titolare, circa il fatto che non possano derivare rischi dalla violazione.. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34 del GDPR, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del D.Lgs 196/2003. I contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del regolamento. Su questo e su tutta la disciplina in materia, il Comitato europeo della protezione dati (si veda art. 70, paragrafo 1, lettere g) e h) del GDPR) è chiamato a formulare linee-guida specifiche, alle quali sta già lavorando il Gruppo "Articolo 29".

---

4 Art. 20 (Principi applicabili al trattamento di dati sensibili), Art. 21 (Principi applicabili al trattamento di dati giudiziari), Art. 22 (Principi applicabili al trattamento di dati sensibili e giudiziari).

5 Da: http://www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili.

6 Per violazione di dati personali si intende, ai sensi dell'art. 4, comma 1, n. 12 del GDPR, "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.".

7 Considerando 85: una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Si segnalano, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali recentemente pubblicate dal Gruppo "Articolo 29" e attualmente in consultazione pubblica, disponibili qui http://ec.europa.eu/newsroom/document.cfm?doc_id=47741.

I Titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (art. 33, par. 5 del GDPR); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del D.Lgs. 196/2003. È, pertanto raccomandabile (nonché necessario) che i Consigli dell'Ordine adottino le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Linee guida CCBE
http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf