Ordine dei Consulenti in Proprietà Industriale

Il Consiglio

Agli Iscritti /studi e società

Il Consiglio dell'Ordine dei Consulenti in Proprietà Industriale, a seguito delle nuove diposizioni sulla privacy di cui al D.lgs 196/2003 come novellato dal D.lgs. 101/2018, ha ritenuto opportuno incaricare ***ICT Legal Consulting, Studio Legale Associato Balboni Bolognini & Partners (ICT Legal Consulting)*** al fine di chiarire il ruolo che i Consulenti in Proprietà Industriale debbano assumere relativamente alla normativa sulla privacy nell'erogazione dei servizi professionali regolati dal Codice della Proprietà Industriale.

Si riporta dunque di seguito, il Memorandum redatto dall'Avv. Nicola Franchetto di ICT Legal Consulting.

Indice

INTRODUZIONE

Il quesito posto

Il presente breve memorandum ("**Memo**") è stato richiesto a seguito di alcune richieste di chiarimento ricevute da professionisti iscritti all'Albo ("**Iscritti**") inerenti al ruolo privacy del consulente nello svolgimento di incarichi professionali regolati dal Codice di Proprietà Industriale ("**CPI**").

Il Memo ha lo scopo di analizzare l'inquadramento dell'Iscritto con riferimento alla normativa in materia di protezione dei dati personali, in particolare comprendere se, nello svolgimento della propria attività, tale soggetto debba considerarsi come un titolare del trattamento ai sensi dell'art. 4.7 del Regolamento (UE) 679/2016 (di seguito: "**Regolamento**"), ovvero come responsabile del trattamento ai sensi del medesimo articolo, punto 8.

Via Napo Torriani, 29 - 20124 MILANO - Tel. 02 55 185 144 - Fax 02 54 122 066
consiglio@ordine-brevetti.it www.ordine-brevetti.it

Sulla base del corretto inquadramento, il Memo fornirà altresì l'elenco dei principali adempimenti che gli Iscritti (o una società tra professionisti o una associazione professionale di cui fa parte l'Iscritto) devono intraprendere per essere conformi a quanto previsto dal Regolamento.

Metodologia

La prima parte del Memo è dedicata a spiegare agli Iscritti le principali nozioni privacy e le differenze tra il ruolo di titolare del trattamento e di responsabile del trattamento.

Presa contezza delle differenze, il Memo le calerà sul ruolo svolto in pratica dall'Iscritto, facendo i dovuti *distinguo* a seconda della forma giuridica assunta dall'Iscritto (es. ditta individuale o società di capitali) nonché sul diverso tipo di attività svolta (es. mandatario marchi o domiciliatario).

Il Memo si chiude con una tabella riassuntiva delle evidenze emerse, di modo che possa fungere da rapido *take away* privacy per gli Iscritti.

I diversi ruoli privacy degli Iscritti

Il titolare e il responsabile: definizioni e differenze

Come noto, ai sensi dell'art. 4.7 e 4.8 del Regolamento, per titolare del trattamento si intende la «*persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*» ("**Titolare**"); mentre per responsabile del trattamento si intende «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*» ("**Responsabile**").

In modo atecnico ma forse più semplice da capire, si è soliti riferirsi al Responsabile come colui che svolge servizi/attività per conto del Titolare adeguandosi alle istruzioni fornite da quest'ultimo.

Seguendo questa linea di pensiero, la distinzione tra Titolare e Responsabile appare piuttosto semplice, soprattutto nei casi più comuni e "di scuola" (es. i fornitori di servizi/applicativi IT come gli hosting provider, i fornitori di CRM, HR management; quelli che generano e inviano buste paga o e-mail/lettere di eventi/marketing per conto del Titolare) dove spesso è il fornitore stesso ad auto-dichiararsi mero fornitore di servizi e dunque Responsabile; in altri casi, invece, tale distinzione non è immediata.

Quando questo accade, è necessario richiamarsi ai fattori indicati dall'ex Gruppo di Lavoro Articolo 29 - denominato a partire dal 28 maggio 2018 "*European Data Protection Board*" o "**Garanti Europei**" - nell'Opinion 1/2010 on the concepts of controller and processor ("**Opinion**")[1] che, benché risalente nel tempo e modulato sulla disciplina della Direttiva 95/46/CE, contiene tuttora le indicazioni "madri" su come distinguere i ruoli. In estrema sintesi, per capire se nel caso concreto si è di fronte ad un Titolare o Responsabile è necessario isolare ed analizzare 2 fattori:

[1] Il testo preso in considerazione per la stesura del presente Memo è la versione ufficiale in lingua inglese e non quella italiana in cui è sono stati erroneamente tradotti l termini "controller" "responsabile" e il termine "processor" in "incaricato" generando nel tempo interpretazioni forvianti.

Chi ha **determinato**/dato origine al trattamento[2] di dati personali[3];
Chi determina le **finalità** e/o le **modalità** del trattamento.

Secondo i Garanti Europei, con il primo fattore si cerca di "**determinare**" per quale ragione il trattamento abbia luogo e chi abbia deciso di porlo in essere. Come si è ricordato più sopra, il Titolare è colui che è competente a decidere sia *l'an* che il *quantum* del trattamento, e tale competenza va verificata attraverso un'analisi delle circostanze di fatto, piuttosto che su predeterminazioni formali[4] (ad esempio, quelle che si leggono su alcune informative o contratti non sempre precisi o chiari sui ruoli e le rispettive obbligazioni).

Il fatto che un soggetto sia autonomo nel dare origine ad un trattamento, continuano i Garanti Europei, può derivare da tre situazioni[5]:

(i) dalla legge, quando è quest'ultima a stabilire che un determinato soggetto, nell'ambito di determinate operazioni di trattamento, agisce come titolare (es. l'Ordine è, per legge istitutiva del CPI, Titolare dei dati personali trattati degli Iscritti all'Albo);

(ii) da competenza implicita (*implicit competence*), che i Garanti Europei individuano nei casi in cui la capacità di determinare il trattamento non sia esplicitamente sancita dalla legge, ma derivi comunque, implicitamente, da previsioni normative o da prassi consolidate in varie aree quali quella giuslavoristica (il datore di lavoro rispetto ai dati dei dipendenti), commerciale (il venditore rispetto ai dati dei propri clienti) ecc., dove i ruoli tradizionali/civilistici assumono un significato anche dal punto di vista del trattamento dei dati;

(iii) da circostanze di fatto, la cui analisi può prendere in considerazione gli accordi contrattuali tra i soggetti coinvolti, ma non esserne influenzata in maniera decisiva se l'allocazione dei ruoli privacy a livello contrattuale non riflette le effettive circostanze di fatto (es. il fatto che un contratto per la stampa e l'invio di buste paga non indichi la società acquirente di questo servizio come Titolare, non significa che quella società non sarà l'effettivo il titolare dei dati forniti).

[2] «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 (cfr. Art. 4(2) Regolamento).

[3] «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (cfr. Art. 4(1) Regolamento).

[4] Opinion 1/2010, p. 8.

[5] Opinion 1/2010, p. 10.

Del resto, si consideri che la normativa di derivazione europea (dunque anche il GDPR e le ulteriori fonti europee rilevanti in ambito privacy) è tipicamente caratterizzata da un approccio sostanzialistico, tale per cui la sostanza – il dato fattuale - è prevalente rispetto alla forma, ancorché la stessa venga contrattualizzata tra le

parti. Ne deriva che ove un'allocazione dei ruoli privacy *formale* non rispecchi le circostanze *fattuali*, la prima soccomberà a favore della seconda.

Ciò posto, il requisito dell'autonomia nella determinazione del trattamento va inteso con esclusivo riferimento alla normativa in materia di protezione dei dati personali e non deve essere confuso con altri principi di diritto, es. quelli sulla proprietà intellettuale[6], precisano i Garanti Europei. Ad esempio, il fatto di essere titolare di un diritto di proprietà industriale, come potrebbe essere un marchio o un brevetto su un software, non significa necessariamente essere anche il Titolare dei dati personali raccolti utilizzando quel marchio o quel software.

Una volta compreso chi ha dato origine al trattamento, il secondo fattore per capire se un soggetto è Responsabile o Titolare prevede la verifica su chi decide "**mezzi e finalità del trattamento**". L'Opinion dei Garanti Europei riporta testualmente le correnti definizioni di "purpose"[7] e di "means"[8]. Le "finalità" si possono definire come il risultato che ci si prefigge di raggiungere o che guida le azioni che vengono intraprese; mentre i "mezzi" come il modo attraverso il quale il risultato viene ottenuto. In altre parole, le finalità rappresentano il "perché" del trattamento, i mezzi il "come" ("why" and "how").

Il peso da dare alle finalità (perché) e ai mezzi (come) del trattamento dipende dal particolare contesto in cui il trattamento è posto in essere e deve essere valutato assumendo un approccio pragmatico: l'elemento della discrezionalità nella definizione del "perché" del trattamento dovrebbe avere un peso preponderante, ed anzi la determinazione delle finalità del trattamento dovrebbe senz'altro far scattare l'inquadramento di un soggetto come Titolare; viceversa, la determinazione dei mezzi potrebbe comportare l'inquadramento come Titolare solo nel caso in cui il soggetto determini davvero elementi essenziali dei mezzi, quali la durata del trattamento, quali dati trattare, a chi darvi accesso ecc.

È ben possibile infatti che gli aspetti tecnici ed organizzativi del trattamento siano demandati integralmente ad un Responsabile in quanto esperto tecnico (es. le misure di sicurezza di un servizio in cloud, la modalità di trasmissione dei dati dei dipendenti per la creazione delle buste paga, le modalità di accesso ad un sistema di posta elettronica sul web), senza spostare tuttavia la titolarità dei dati ivi trattati.

Compresi i criteri suggeriti dai Garanti Europei, per comprendere il ruolo privacy degli Iscritti occorre anzitutto analizzarne le raccolte dati e le specifiche funzioni svolte.

Quando l'Iscritto agisce in qualità di titolare del trattamento

Stante le regole generali sopra riportate, l'Iscritto risulta Titolare ogni qualvolta dia origine o determini l'inizio di un trattamento. Questo avviene almeno nei seguenti casi:

[6] Cfr. Opinion p. 9 "*The concept of controller should not be prejudiced by other - sometimes colliding or overlapping - concepts in other fields of law, such as the creator or the right holder in intellectual property rights. Being a right holder for intellectual property does not exclude the possibility of qualifying as "controller" as well and thus be subject to the obligations stemming from data protection law.*".
[7] Cfr. Opinion p. 9 *"an anticipated outcome that is intended or that guides your planned actions".*
[8] Cfr. Opinion p. 9 "*how a result is obtained or an end is achieved".*

quando tratta dati dei propri dipendenti e collaboratori (se presenti): l'Iscritto è Titolare dei dati personali dei dipendenti in quanto datore di lavoro e dei collaboratori in qualità di loro committente/cliente;

quando raccoglie i dati dei clienti per inserirli nella propria anagrafica, dunque anche per ottemperare ad obblighi di legge: l'Iscritto è Titolare dei dati personali dei clienti persone fisiche (o dei legali rappresentanti firmatari per le persone giuridiche) che firmano il mandato/contratto di consulenza e dunque anche per le finalità di fatturazione, obblighi di identificazione per la normativa antiriciclaggio ecc.;

quando raccoglie dati ad eventi: l'Iscritto che raccoglie dati personali (anche attraverso lo scambio di biglietti da visita) è Titolare dei dati raccolti e, in assenza di idonea informativa, potrà utilizzarli solo per ricontatti del tutto personali e non collegati a finalità promozionali o marketing della società/associazione professionale di cui fa parte, i cui trattamenti devono basarsi necessariamente su una previa informativa e consenso (per il marketing) ai sensi degli art. 13 Regolamento e art. 130 Codice Privacy).

Si precisa che qualora il mandato/contratto di consulenza sia sottoscritto tra il cliente e una società tra professionisti o una associazione professionale di cui fa parte l'Iscritto o nei casi in cui l'Iscritto stia raccogliendo dati per conto di quest'ultima, il Titolare dei dati raccolti (e dunque anche degli eventuali obblighi normativi/fiscali inerenti al mandato) non sarà l'Iscritto, bensì la stessa società tra professionisti o una associazione professionale per conto della quale si svolge l'attività di trattamento.

In tali casi, l'Iscritto non è soggetto agli obblighi di un Titolare e sarà legittimato a trattare i dati personali del cliente della società tra professionisti o una associazione professionale (il vero Titolare), solo qualora quest'ultima abbia provveduto alternativamente a nominare l'Iscritto quale:

persona autorizzata a trattamento dei dati personali (il cd. "incaricato" secondo la precedente normativa) ai sensi degli artt. 28(3)(b), 29 Regolamento ed eventualmente 2-quaterdieces del D.lgs 196/2003 come novellato dal D.lgs. 101/2018 ("**Codice Privacy**")[9];

nominare l'Iscritto quale Responsabile tramite un contratto per il trattamento dei dati ai sensi dell'art. 28 Regolamento.

La scelta tra queste due opzioni alternative risiederà nella possibilità o meno per l'Iscritto di determinare i mezzi con cui trattare i dati personali del cliente della società tra professionisti o una associazione professionale (il Titolare): se nel trattare i dati oggetto dell'incarico l'Iscritto ha un'organizzazione di mezzi propria (es. laptop, smartphone, e-mail e archivi fisici) come nel caso di un Iscritto con più collaborazioni diverse, allora dovrà essere nominato Responsabile; in caso contrario – ossia se non vi è margine di discrezionalità per quest'ultimo di determinare "come" trattare i dati del cliente finale (ad esempio perché mezzi come smarpthone e laptop

[9] La versione consolidata è reperibile al seguente link: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29 ultimo accesso (22 marzo 2019).

vengono forniti e messi in sicurezza dalla società/associazione che ha ricevuto l'incaricato), dovrà essere nominato persona autorizzata.

Quanto sopra riportato non deve essere confuso con il diverso caso in cui il mandato/incarico professionale sia dato congiuntamente a più Iscritti (dunque senza l'intermediazione di uno studio o associazione professionale). In questi casi, gli Iscritti agiranno in qualità di contitolari del trattamento ai sensi dell'Art. 26 Regolamento, dovendo adempiere agli obblighi ivi previsti (es. conclusione di un accordo di contitolarità e conferimento di un'informativa congiunta ai sensi dell'art. 13 Regolamento).

I principali adempimenti del Titolare

Per tutti i casi citati più sopra a titolo esemplificativo e non esaustivo in cui l'Iscritto (o la società tra professionisti o una associazione professionale per cui lavora il primo) risulta essere Titolare, quest'ultimo dovrà assicurarsi *inter alia* di quanto segue:

avere un modulo/form di raccolta dati che rispetti il principio di minimizzazione del dato (es., non richiedere l'inserimento di dati che non siano strettamente necessari);

non aver reso come obbligatorio (es. tramite asterischi) l'inserimento di più dati di contatto di quelli necessari (es., se l'unica finalità perseguita dall'Iscritto è avere un punto di contatto con il cliente a cui inviare le fatture/comunicazioni di servizio, potrà essere reso obbligatorio il campo "e-mail" ma non anche il campo "telefono" o "mobile");

aver ragionato su quali sono le finalità per cui si intendono trattare i dati (es. fornitura di una consulenza, adempimento di obblighi fiscali, marketing) e riflettere queste e le altre informazioni nell'informativa agli interessati ex art. 12-14 Regolamento (nel caso di mandato congiunto con altro Iscritto senza l'intermediazione della società/associazione professionale, tale informativa dovrà essere data congiuntamente dagli Iscritti anche sulla base di quanto concordato internamente tra loro nell'accordo di contitolarità ex art. 26 Regolamento);

ove il trattamento scelto rientri nella cd. blacklist[10] del Garante per la protezione dei dati personali, aver proceduto preliminarmente a svolgere una valutazione sul trattamento dei dati personali (cd. DPIA);

aver valutato le basi giuridiche che supportano quei trattamenti (es. per la fornitura di un servizio l'art. 6.1.b Regolamento; per l'adempimento ad obblighi normativi l'art. 6.1.c Regolamento ecc.), raccogliendo il consenso ove necessario (es. per finalità di marketing) o valutando la presenza di un legittimo interesse;

aver aggiornato il registro dei trattamenti ex art. 30.1 Regolamento[11];

[10] Cfr. "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 [9058979]" e rispettivo Allegato 1 disponibile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979 (ultimo accesso 22 marzo 2019).

aver implementato idonee misure di sicurezza (si ricorda che l'Allegato B Codice Privacy è stato abrogato, lasciando al Titolare la scelta di quali misure adottare ai sensi dell'art. 32 Regolamento);

aver nominato eventuali persone autorizzate al trattamento (es. dipendenti/collaboratori);

aver nominato eventuali Responsabili ingaggiati per quel trattamento, assicurandosi di aver fornito idonee istruzioni su come trattare i dati personali (es. con riferimento ai trasferimenti di dati all'estero o alla possibilità per il Responsabile di nominare altri sub-responsabili).

Quanto sopra deve essere letto con rimando alla disciplina privacy *pro tempore* vigente (compresi i provvedimenti e le linee guida dell'Autorità Garante) e alla luce delle seguenti precisazioni:

oltre a quelli indicati in via principale qui sopra per comodità del lettore, sul Titolare incombono altri adempimenti (es. eventuale nomina di un DPO, formazione, rispetto degli adempimenti per il trasferimento dei dati fuori dallo Spazio Economico Europeo ecc.);

in caso di violazione della normativa, sul Titolare incombono sanzioni che possono arrivare fino al 4% del fatturato nell'anno fiscale precedente (cfr. art. 83 Regolamento);

la persona autorizzata potrà essere chiamata a rispondere di eventuali danni prodotti solo in regresso e solo qualora abbia violato le istruzioni fornite dal Titolare nella lettera di nomina fatta sottoscrivere. Il Responsabile eventualmente ingaggiato per il trattamento risponde in via principale o in regresso solo qualora abbia violato le disposizioni/istruzioni indicate dal Titolare nel contratto per il trattamento dei dati personali. Da qui ne consegue che sul Titolare spettano tanto oneri in *eligendo* (es. verifica preliminare sui fornitori/software che si vogliono implementare) quanto quelli in *vigilando* (es. formazione del personale ed eventuali audit sui fornitori ingaggiati).

Quando l'Iscritto agisce in qualità di responsabile del trattamento

Nel precedente paragrafo si è evidenziato come i casi in cui l'Iscritto (o la società tra professionisti o una associazione professionale per cui lavora il primo) risulti essere Titolare dei dati personali raccolti non sono molto diversi da quelli di qualsiasi altra attività in cui si raccolgono dati direttamente da soggetti interessati (es. un'agenzia, un negozio, un sito internet).

Del tutto diversa è invece la situazione di quando l'Iscritto (o la società tra professionisti o una associazione professionale per cui lavora il primo) debba essere considerato Responsabile, in cui molto spesso si è portati a pensare che le caratteristiche di professionalità e indipendenza - prescritte nello svolgimento di un'attività regolamentata da parte di una legge istitutiva e da un codice deontologico - debbano rendere l'Iscritto "svincolato" da istruzioni di qualunque genere, soprattutto se provenienti dal proprio cliente/Titolare. Si ritiene che questa semplificazione possa essere quantomeno limitativa se non foriera di una non corretta applicazione dei ruoli privacy.

[11] Per le eccezioni alla tenuta del registro si legga anche il "Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR" dei Garanti Europei disponibile al seguente link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045 (ultimo accesso 22 marzo 2019).

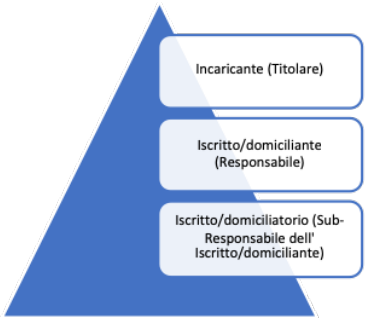
Con conferimento alla fattispecie di un mandato/incaricato professionale, si ritiene che l'Iscritto (o la società tra professionisti o una associazione professionale se l'incarico è sottoscritto da quest'ultima) debba ragionevolmente essere considerato come un Responsabile per conto del mandante (per comodità di lettura di seguito solo "**Incaricante**") per i seguenti motivi:

chi dà origine al trattamento dei dati personali è l'Incaricante attraverso il mandato e non l'Iscritto o la società tra professionisti o un'associazione professionale (1° criterio dei Garanti Europei);
chi determina le finalità (il "perché") del trattamento è l'Incaricante (es. necessità di registrare un marchio); mentre all'Iscritto (o alla società tra professionisti o un'associazione professionale) viene lasciata solo la determinazione dei mezzi (il "come", es. procedere o meno ad una ricerca di anteriorità prima della registrazione del marchio) non potendo trattare i dati raccolti per proprie finalità (2° criterio dei Garanti Europei);

le istruzioni sul trattamento trasmesse dall'Incaricante all'Iscritto (o alla società tra professionisti o l'associazione professionale) tramite un contratto per il trattamento ex art. 28 Regolamento, non inficiano in alcun modo sulla professionalità ed indipendenza dell'Iscritto. Questo perché il trattamento dei dati personali è considerata attività *in re ipsa* pericolosa ai sensi dell'art. 2050 c.c., dunque dare istruzioni ad un avvocato/ingegnere/primario di sala operatoria su come trattare "materiale pericoloso" appartenente ad un altro soggetto (il cliente/Titolare) non è diverso da qualsiasi altra istruzione che queste figure già ricevono in ambito di sicurezza sul lavoro/incendio/piani di evacuazione che, al pari della prima, non inficiano sull'indipendenza o autonomia dell'attività svolta, ma richiedono solo maggiori e più specifiche cautele per il cliente;

soprattutto nell'ambito della tutela della proprietà intellettuale, dove riservatezza e celerità nell'esecuzione del mandato sono fattori fondamentali per la competitività del cliente, il contratto per il trattamento dei dati ex art. 28 Regolamento è l'unico mezzo a disposizione con il quale l'Incaricante può verificare/imporre specifiche misure di sicurezza, vincoli sul trasferimento di dati all'estero o sull'uso di altri sub-Responsabili che potrebbero non essere graditi dall'Incaricante (es. Microsoft che richiede la registrazione di un brevetto per una nuova tecnologia di hosting e l'Iscritto salva i dati dell'inventore e di tutto il materiale per la registrazione su server di un competitor hosting di Microsoft).

L'inquadramento come Responsabile appena esposto deve ritenersi applicabile anche nel caso in cui l'Iscritto (o la società tra professionisti o l'associazione professionale) svolga il ruolo di domiciliatario per conto di altro collega. In questi casi, pare corretto inquadrare l'Iscritto quale sub-Responsabile ai sensi dell'art. 28(4) Regolamento del collega (Responsabile) che gli ha delegato l'esecuzione di parte dell'incarico del suo cliente (Titolare).



In tali casi, sarà onere del collega domiciliante (quando intende domiciliare parte dell'attività) ottenere l'autorizzazione (preferibilmente generale) dal cliente (Titolare) all'impiego di sub-responsabili ai sensi dell'art. 28(2)(4) Regolamento. Lo stesso dovrà applicarsi quando è lo stesso Iscritto (o la società tra professionisti o l'associazione professionale) a voler delegare a terzi colleghi parte dell'incarico ricevuto dal proprio cliente/Titolare.

A conferma dell'impostazione che vede l'Iscritto (o la società tra professionisti o l'associazione professionale che ha ricevuto l'incarico) quale Responsabile, e dei criteri dei Garanti Europei, vi è una recente pronuncia dell'Autorità Garante per la protezione dei dati personali che ha risposto in modo chiaro ad un quesito presentato dall'associazione di categoria dei consulenti del lavoro, in cui si paventava che tra quest'ultimi e il cliente che conferisce l'incarico si instaurasse un rapporto di titolarità o al più contitolarità in quanto i primi avrebbero "*piena autonomia di decisione […] nella scelta delle modalità e dei mezzi (anche tecnologici) ritenuti più opportuni, così come nella scelta dei collaboratori cui affidare il trattamento*"[12].

Come precisato più sopra, la scelta dei mezzi e dei collaboratori determina il "come" e non la ragione d'essere o la finalità del trattamento (il "perché"), come confermato dalla stessa Autorità di cui si riportano gli estratti essenziali applicabili in via analogica agli Iscritti e in cui sono state sostituite le parole "datore di lavoro" e "consulente del lavoro" con rispettivamente "cliente" ed "Iscritto" per comodità di lettura:

Infatti, in base alla disciplina di riferimento è pur sempre il [cliente] ad affidare al [Iscritto] il relativo incarico (conferendo anche materialmente, se del caso, la relativa documentazione: […] e peraltro ciò non lo esime per espresso volere del legislatore ed anche a garanzia del [Iscritto] dalla assunzione della responsabilità prevista dall'ordinamento in caso di violazione degli obblighi posti in materia […]. D'altra parte [l'Iscritto], nello svolgimento della propria qualificata attività professionale, opererà applicando le discipline di settore e le regole deontologiche pertinenti. L'affidamento dell'incarico al [Iscritto] avverrà, anche in base alle norme di diritto comune applicabili, attraverso la sottoscrizione di un "contratto o altro atto giuridico" stipulato concordemente dalle parti tenendo conto dei compiti in concreto affidati, del contesto, delle finalità e modalità del trattamento […]

Qualora il [Iscritto] si avvalga normalmente di collaboratori di propria fiducia […] questi, in base alle concrete operazioni di trattamento affidate, potranno operare sotto la sua diretta autorità e in base alle istruzioni impartite, configurando il rapporto preso in considerazione dall'art. 29 del Regolamento. Più specificamente, in base all'art. 2-quaterdecies del Codice il responsabile può prevedere che "specifici compiti e funzioni connessi al trattamento siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità" Oppure, diversamente, i collaboratori potranno assumere in concreto il ruolo di subresponsabili, qualora sia demandata "l'esecuzione di specifiche attività di trattamento per conto del titolare" (v. art. 28, par. 4 del Regolamento). In tale ipotesi, anche al fine di impedire l'elusione della norma che prevede che il titolare [cliente] debba ricorrere a soggetti che forniscano specifiche garanzie di affidabilità, competenza e organizzazione, il paragrafo 2 dell'art. 28 prevede che il relativo atto di incarico debba essere autorizzato, anche in via generale (dunque non necessariamente specifica) dal titolare".

[12] Si veda "Risposta a un quesito relativo al ruolo del consulente del lavoro dopo la piena applicazione del Regolamento (UE) 679/2016" disponibile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9080970 (ultimo accesso 22 marzo 2019).

Il regolamento ha inoltre attribuito direttamente al responsabile del trattamento compiti specifici in ordine alla individuazione e predisposizione delle idonee misure di sicurezza adeguate al rischio, attraverso misure tecniche ed organizzative (v. art. 32 del Regolamento). Al [Iscritto] che operi in qualità di responsabile del trattamento è dunque attribuito un apprezzabile margine di autonomia (e correlativa responsabilità) nella individuazione dei sistemi e delle misure idonee a garantire la sicurezza dei dati gestiti nei propri archivi.

[…] qualora il [Iscritto] agisca in veste di responsabile del trattamento, la base normativa che legittima il trattamento dei dati personali, […] va individuata in capo al suo cliente (ovverosia il [cliente]/titolare) ai sensi dell'art. 9, par. 2, lett. b), del Regolamento: infatti, la legittimità del trattamento si "trasferisce" alle operazioni svolte dal [Iscritto] in ragione del contratto di sua designazione a responsabile del trattamento"[13].

Quanto fin qui esposto si intende applicabile in un modo che ci pare – sulla base di quanto sopra esposto - pacifico a tutte le attività stragiudiziali svolte da tutti gli Iscritti (o dalle società tra professionisti o associazioni professionali) siano essi ingegneri/avvocati/mandatari esteri presenti nell'Albo.

Discorso diverso deve essere fatto invece qualora oggetto dell'incarico sia **attività giudiziale**, ad esempio di fronte all'Ufficio Marchi Brevetti o a tribunali amministrativi/civili/penali per la tutela della proprietà intellettuale dei propri clienti, per i quali non vi è opinione comune o una chiara pronuncia da parte dell'Autorità Garante.

Secondo una prima teoria, supportata da un parere del Consiglio Nazionale Forense[14] dall'Autorità Garante inglese (*Information Commissioner's Office*)[15] e all'Opinion dei Garanti Europei si ritiene che gli avvocati (presenti come categoria all'interno degli Iscritti) debbano essere considerati Titolari quando svolgono attività giudiziali (i.e., "*Un avvocato rappresenta un suo cliente davanti al giudice, e nell'ambito di tale funzione tratta dati personali collegati al caso del cliente. La base legale per poter utilizzare le informazioni necessarie è il mandato dal cliente. Tale mandato, tuttavia, non verte sul trattamento di dati bensì sulla rappresentanza in giudizio, attività per la quale queste professioni hanno tradizionalmente la propria base legale. Tali professioni devono quindi essere considerate come "responsabili del trattamento"* [da leggersi come "titolari del trattamento per un disallineamento nella traduzione da inglese a italiano][16] *indipendenti per quanto riguarda il trattamento dei dati svolto nell'ambito della rappresentanza legale del cliente*" cfr. Opinione 1/2010 dei Garanti Europei, p. 29).

Le menzionate opinioni, tuttavia, non sembrano chiarire in modo esaustivo le ragioni/criteri privacy utilizzati per sostanziare il detto inquadramento, né soprattutto sembrano prendere in considerazione il fatto che

[13] *Ibidem*.
[14] Si veda "Il GDPR e l'avvocato" disponibile al seguente link: https://www.consiglionazionaleforense.it/documents/20182/445621/IL+GDPR+E+L%27AVVOCATO/ef231b75-2066-43df-8d88-570bf0ea98b3 (ultimo accesso 22 marzo 2019).
[15] Si veda punto 25 e seguenti del "Data controllers and data processors:what the difference is and what the governance implications are" disponibile al seguente link: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf (ultimo accesso 22 marzo 2019).
[16] Si precisa che la parola inglese "controller" è stata erroneamente tradotta in italiano con il termine "responsabile del trattamento" creando nel tempo interpretazioni fuorvianti. Il termine "responsabile del trattamento" in questo passaggio deve essere sostituito con "titolare del trattamento". Per conferma si faccia riferimento alla versione inglese dell'Opinione in esame.

l'attività dell'avvocato può estrinsecarsi in diverse forme e attività: avvocato in quanto consulente stragiudiziale; avvocato nel suo ruolo di procuratore in giudizio/arbitrato/ADR; avvocato come mandatario ex CPI; avvocato come consulente del lavoro (quest'ultimo già inquadrato come Responsabile dall'Autorità Garante e non come Titolare nella pronuncia sopra citata) ecc..

Una seconda possibile teoria, privilegiata da chi scrive alla luce dei criteri generali dei Garanti Europei e della *ratio* alla base della pronuncia dell'Autorità Garante nel caso dei consulenti del lavoro, ritiene che, anche per un'attività giudiziale di fronte ad organi amministrativi/giurisdizionali, l'Iscritto (o la società tra professionisti o associazione professionale incaricata) agisca fattualmente comunque come Responsabile per i seguenti motivi, già in parte richiamati più sopra:

chi dà origine al trattamento dei dati personali è l'Incaricante tramite mandato e non l'Iscritto/i o la società tra professionisti o una associazione professionale (1° criterio dei Garanti Europei);

chi determina le finalità (il "perché") del trattamento è l'Incaricante tramite una richiesta nella maggior parte dei casi atecnica ma chiara nella sua ragion d'essere (es. necessità di registrare/tutelare un marchio o una situazione di fatto meritevole di tutela) (2° criterio dei Garanti Europei). Tale richiesta assume la forma di un mandato/incarico ad agire per conto e/o in nome dell'Incaricante in cui si specifica non solo "*rappresentanza in giudizio, attività per la quale queste professioni hanno tradizionalmente la propria base legale",* ma anche i poteri di azione conferiti all'avvocato Iscritto (es. il potere di agire in tutte le fasi del giudizio o solo in quella di merito; il potere di transigere; il potere di incaricare solo l'Iscritto *intuitu personae,* o più Iscritti, oppure ancora tutti gli Iscritti della società/associazione professionale a cui l'Incaricante si è rivolto). All'Iscritto resta solo e tutta la determinazione tecnico/legale/consulenziale sui mezzi e le strategie (es. suggerire di registrare marchi cd. difensivi a supporto della registrazione principale; consigliare la registrazione per più categorie nella classificazione di Nizza; raccomandare un'opposizione alla registrazione; produrre prove e testimoni che ritiene siano utili per cliente ecc.) da impiegare o meno per soddisfare nel migliore dei modi le finalità indicate dall'Incaricante durante la fase di studio del caso e consolidate nel mandato. Chi scrive ritiene che la discrezionalità posta in capo all'Iscritto non sia "piena" (intesa come discrezionalità nel merito), quanto piuttosto una discrezionalità prettamente tecnica, nel senso tecnico/amministrativo del termine. Ossia una discrezionalità che non riguarda appunto la scelta di merito (è il cliente che chiede ad es. di registrare un marchio, determinando la finalità per la quale conferisce mandato/incarico) ma unicamente i passaggi tecnici/amministrativi richiesti per perseguire tale finalità. Non essendo l'Incaricante un soggetto *peritus*, per ovvie ragioni dovrà affidarsi alle competenze dell'Iscritto, lasciandogli una discrezionalità sulle scelte tecniche (es. procedimenti, atti, autorizzazioni) necessarie per poter portare a termine il mandato. La stessa situazione che del resto si verificherebbe per un imprenditore che deve nominare quale Responsabile una software house per la gestione dei sistemi informatici: nessuno dubiterebbe circa il fatto che sebbene sia la software house a proporre autonomamente i mezzi tecnici per la conservazione/gestione dei dati[17], questa possa ciò nonostante conservare il ruolo di Responsabile. Inoltre, si noti che in assenza di mandato o fuori dal suo perimetro, l'Iscritto nulla può, difettando della capacità di agire per conto dell'Incaricante;

[17] Per quanto sia l'art. 28 Regolamento a porre sul Titolare l'obbligo di determinare le misure di sicurezza che il Responsabile dovrà applicare per il trattamento dei dati, non vi è chi non veda come, nei primi mesi di applicazione dell'art. 32 Regolamento, di fatto è il Responsabile, perito del mestiere, ad indicare/proporre le proprie misure di sicurezza lasciando ex post al Titolare la facoltà di accettarle o meno.

all'interno del mandato, l'Iscritto può determinare tutti i mezzi che più soddisfano le finalità determinate dall'Incaricante nel rispetto del codice deontologico, ma si tratta sempre di mezzi, non finalità. Sebbene anche l'Iscritto possa dare "suggerimenti" di merito, sarà sempre l'Incaricante a decidere se procedere o meno perché tali suggerimenti potrebbero comportare assunzioni di rischio ovvero oneri economici che l'Iscritto non può (e non vuole) assumere. In questo senso, nulla di un contratto per il trattamento dei dati ex art. 28 Regolamento pare porsi in contrasto con l'autonomia tecnica dell'Iscritto in sede giudiziale/amministrativa:

non si ritiene sia in contrasto con l'obbligo di riservatezza deontologica (che anzi è rafforzato con l'inserimento di specifiche misure che l'Incaricante potrebbe - ma anche dovrebbe e vorrebbe - imporre solo ad un Responsabile e non ad un Titolare; cfr. *infra*);

non si ritiene sia in contrasto con la necessaria e qualificante discrezionalità tecnica dell'Iscritto perché ha ad oggetto istruzioni sul trattamento dei dati che sono slegate dalle scelte professionali di merito;

non si ritiene sia in contrasto con le norme deontologiche/professionali/fiscali che impongono al prestatore la conservazione di (parte dei) dati oggetto della prestazione, trattandosi invero di attività permesse nei limiti previsti dalla legge (cfr. Art. 28(3)(g): ["*Il contratto o altro atto giuridico prevede … che il responsabile del trattamento] su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati*");

non si ritiene sia in contrasto ed anzi supporterebbe la parità di trattamento tra Iscritto - non avvocato ed Iscritto avvocato.

Se si seguisse la prima teoria (quella che vede l'Iscritto quale Titolare), si arriverebbe al risultato, apparentemente paradossale e fattualmente impraticabile, che in un caso di registrazione di brevetto, l'Iscritto (la società tra professionisti o associazione professionale incaricata) o gli Iscritti (in caso di mandato disgiunto) dovrebbero non solo presentare un'informativa privacy ex art. 13 Regolamento al cliente persona fisica (legale rappresentante per le persone giuridiche) che ha commissionato la registrazione, ma anche conferire un'informativa ex art. 14 Regolamento all'inventore i cui dati sono stati forniti dal cliente per la brevettazione (salva l'applicazione delle eccezioni a questo adempimento). Lo stesso dicasi per i soggetti i cui dati sono comunicati dal cliente per l'esecuzione della prestazione professionale (es. dipendenti/funzioni del cliente).

Ancora, se si percorresse questa via, il cliente persona fisica o il legale rappresentante dell'interessato (tecnicamente cd. interessati) non avrebbero la possibilità di chiedere all'Iscritto (o alla società tra professionisti o associazione professionale incaricata) di applicare ai dati trattati per l'esecuzione del servizio specifiche precauzioni e misure di sicurezza, il divieto o meno di trasferire dati all'estero, il divieto o meno di utilizzare certi Responsabili, il dovere di fornire evidenze di compliance, il dovere di collaborazione in caso di data breach ecc. (cfr. Art. 28 Regolamento), con l'evidente rischio di mettere a repentaglio anche gli investimenti interni del cliente per lo sviluppo e la tutela del proprio asset immateriale. In questo senso, la sottoscrizione di un contratto per il trattamento dei dati può essere letta come l'estrinsecazione pratica, puntuale e più facilmente rafforzabile, di un obbligo di segretezza e diligenza professionale già previsti, come principio, dal nostro ordinamento (cfr. art. 1176 c.c. e codici deontologici).

La tesi che giustifica la titolarità sulla base di obblighi di professionalità e indipendenza dei prestatori è sostenuta soprattutto dalle società di revisione contabile, dove non vi è chi non veda come la grandissima mole di dati trattati da quest'ultime durante queste operazioni renda ancora più evidenti le criticità sopra evidenziate. Anche in questi casi, nulla all'interno di un contratto per il trattamento dei dati pare in contrasto

con gli obblighi di professionalità e indipendenza dei revisori. Al contrario, è l'unico modo per impedire una pratica, spesso troppo diffusa anche in altri settori, di *secondary use* dei dati raccolti per la generazione di report o servizi di business information a terzi soggetti dietro una generica "maschera" di "miglioramento dei servizi offerti".

Come anticipato, l'Autorità Garante ha avuto modo di esprimersi sul ruolo dei consulenti del lavoro (applicabile ad avviso di chi scrive in via analogica per l'attività stragiudiziale degli Iscritti) ma non ancora sul ruolo degli avvocati (Iscritti) secondo quanto indicato dal Consiglio Nazionale Forense.

Consigliando di interpellare l'Autorità Garante per confermare l'impostazione assunta in questo Memo, si ritiene - anche a maggior tutela del cliente finale come sopra riportato, finalità che l'Ordine già tutela attraverso altre forme, come la verifica dei requisiti professionali per l'iscrizione all'Albo, la sua conseguente diffusione, la previsione di sanzioni anche a tutela degli Iscritti – che, oltre ai casi in cui svolge attività stragiudiziale, anche per l'attività giudiziale l'Iscritto (o la società tra professionisti o associazione professionale incaricata) debba ragionevolmente e di regola essere inquadrato come Responsabile.

I principali adempimenti del responsabile

Fatti salvi gli adempimenti di cui al paragrafo 2.2.1 più sopra - per il trattamento dei dati personali del cliente persona fisica e legale rappresentante di persona giuridica che l'Iscritto (o la società tra professionisti o associazione professionale incaricata) svolge in qualità Titolare - si riportano di seguito a titolo esemplificativo e non esaustivo quelli ulteriori previsti i per il ruolo di Responsabile, rimandando sempre per completezza alla normativa pro tempore applicabile che include anche eventuali linee guida e pareri dell'Autorità di Garante:

- individuare le misure di sicurezza che si riescono a garantire per la tutela dei dati del cliente/Titolare (es. la conservazione dei dati in archivi protetti, la cifratura del disco rigido, sistemi di firewall e antivirus, segregazione degli accessi fisici e logici). A tal riguardo si precisa che l'Allegato B del Codice Privacy (contenente misure di sicurezza scritte più di 15 anni fa) è stato abrogato e sostituito da un più oneroso principio di *accountability* nella scelta delle misure di sicurezza (cfr. Artt. 5 e 32 Regolamento), pertanto agli Iscritti compete una seria e documentata riflessione sulle misure di sicurezza a garanzia dei dati personali di clienti, dipendenti e collaboratori che prescinde dal ruolo di Responsabile o Titolare;

- individuare e nominare le persone autorizzate al trattamento dei dati (ex "incaricati") assegnando profili di autorizzazione che rispettino il principio del privilegio minimo (es. un Iscritto non dovrebbe accedere a dati di pratiche non di sua competenza);

- individuare e nominare (sub)Responsabili ai sensi dell'art. 28 Regolamento quei fornitori/software/domiciliatari utilizzati per trattare i dati del cliente (es. fornitori hosting/e-mail su cui sono salvati i dati del cliente) imponendo a questi di rispettare gli stessi obblighi di sicurezza garantiti in prima istanza dall'Iscritto al cliente (es. si pensi ad un domiciliatario che usi un laptop senza password per trattare i dati del cliente dell'Iscritto);

- stipulare un contratto per il trattamento dei dati ai sensi dell'art. 28 Regolamento con il cliente (Titolare) in cui si riportano le misure di sicurezza e l'elenco dei (sub) Responsabili per i quali si richiede l'autorizzazione specifica o generale all'utilizzo ai sensi dell'art. 28(2) Regolamento.

Si precisa che quanto sopra riportato rappresenta solo l'insieme dei principali obblighi del Responsabile senza includere gli eventuali ulteriori adempimenti previsti dal Regolamento (es. mantenere un registro dei trattamenti ex art. 30.2 Regolamento anche a mente del Position Paper dei Garanti Europei, fornire collaborazione con le eventuali richieste dei soggetti interessati, valutazioni di impatto e data breach; individuare le idonee garanzie per il trasferimento dei dati fuori dall'SEE, fornire evidenze di compliance ecc.).

Tabella riassuntiva

Mandato affidato a	Trattamento	Ruolo privacy ricoperto
Iscritto (o società/associazione professionale)	Dati del cliente persona fisica/ legale rappresentante di persona giuridica (es. per adempimenti normativi)	**Titolare**
Più Iscritti per incarico affidato congiuntamente (senza intermediazione della società/associazione professionale)	Dati del cliente persona fisica/ legale rappresentante di persona giuridica (es. per adempimenti normativi)	**Contitolari**
Più Iscritti per incarico affidato disgiuntamente (senza intermediazione della società/associazione professionale)	Dati del cliente persona fisica/ legale rappresentante di persona giuridica (es. per adempimenti normativi)	**Ognuno è autonomo Titolare per la parte di trattamento ad esso affidata**
Iscritto (o la società/associazione professionale)	Esecuzione del mandato stragiudiziale	**Responsabile**
Iscritto (o la società/associazione professionale)	Esecuzione del mandato giudiziale amministrativo	**Titolare/Responsabile**

Il Consiglio dell'Ordine dei Consulenti in Proprietà Industriale