Commissione Informatica COA Bari

VADEMECUM REGOLAMENTO UE 679/2016

COGLI L'ATTIMO

Sommario

Autore: Avv. Adriana Augenti. Con la collaborazione degli Avv.ti Angelo Bianco, Giuseppe Marinelli, Patrizio Galeotti, Giuseppe Valori e Gruppo di lavoro Privacy della Commissione Informatica COA Bari.

1. Premessa

Il presente Vademecum è stato pensato e ideato in seno alla Commissione Informatica del Consiglio dell'Ordine degli Avvocati di Bari. In particolare, al Gruppo di lavoro privacy della ridetta Commissione. È stato pertanto pensato per un pubblico di avvocati, anche se in modo circolare: è infatti corredato di qualche suggerimento per **COGLIERE L'ATTIMO**.

Non ha pretese di esaustività e completezza, né potrebbe averne.

Non ha pretese di esattezza.

I numeri tra parentesi dei vari capitoli e paragrafi indicano il corrispondente articolo del Regolamento cui l'argomento si riferisce. La scelta di non seguire in modo pedissequo l'ordine degli articoli è voluta e ci auguriamo che faciliti ulteriormente la comprensione del testo.

Il formato permette la navigazione interna ed esterna del documento: cliccando sulle voci del sommario o sui numeri dei vari riferimenti contenuti tra parentesi preceduti dalla parola "vedi" si raggiunge il riferimento indicato; cliccando sui titoli dei capitoli o dei paragrafi si viene reindirizzati al sommario; in coda al Vademecum, i link alle **FONTI NORMATIVE**, a un modello di **INFORMATIVA** per studi legali e a un modello di **REGISTRO DI ATTIVITÀ DI TRATTAMENTO** per Studi Legali, entrambi in formato compilabile con relative istruzioni per la compilazione.

2. Cos'è e a chi si rivolge

Il Regolamento Europeo sulla protezione dei dati, meglio noto come GDPR, si applica al trattamento di dati personali automatizzato o meno, salvo che:

a) L'attività svolta non sottostà al diritto UE;
b) L'attività è svolta per disposizioni specifiche di politica estera e sicurezza comune (Titolo V, capo 2, TUE)
c) L'attività è svolta da una persona fisica ed ha carattere esclusivamente personale o domestico;
d) L'attività è svolta da Autorità per la prevenzione o perseguimento di reati o per l'esecuzione di sanzioni penali.

L'**RGPD** (Regolamento Generale sulla Protezione dei Dati) si applica a tutti i trattamenti effettuati sia nell'Unione sia fuori dall'Unione quando:

3. il Titolare o uno dei suoi responsabili abbiano stabilimento in almeno uno degli Stati membri;
4. l'Interessato si trova in uno degli Stati membri.

3. Dato personale (4)

Si definisce come dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile, dal Regolamento definito come **INTERESSATO**.

La casistica delle informazioni utili a identificare un soggetto/persona fisica è molto ampia (art. 4 n. 1). Si considera, ad esempio, dato personale anche un dato biometrico (iride, impronta digitale …) ma anche dati relativi all'ubicazione.

3.1 Dati particolari, reati e condanne penali (9, 10)

Particolare attenzione viene riposta sul trattamento di quella categoria di dati, prima definiti "sensibili", ed ora ampliati e individuati sotto la rubrica dell'art. 9 come **CATEGORIE PARTICOLARI DI DATI PERSONALI**.
Fra questi sono ricompresi quei dati che rivelano, a titolo esemplificativo: origine razziale o etnica; opinioni politiche; convinzioni religiose e filosofiche; appartenenza sindacale; dati genetici; dati biometrici; dati sulla salute; dati sulla vita sessuale; dati sull'orientamento sessuale; dati personali relativi a condanne penali e reati; altri dati personali protetti dal segreto professionale.

Il Regolamento in linea generale **vieta** il trattamento di questi dati, fatte salve alcune eccezioni, tra cui, per quel che qui interessa:

a) presenza di consenso espresso (che deve essere anche inequivocabile) nei soli casi in cui è revocabile secondo la legge nazionale o UE;
b) per l'assolvimento di obblighi o l'esercizio di diritti da parte del titolare in materia di diritto del lavoro e della sicurezza e protezione sociale;
c) è necessario per la tutela di un interesse vitale e l'interessato non è nelle condizioni fisiche o giuridiche di prestare il consenso;
d) è effettuato, con le dovute garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro per il perseguimento di finalità politiche, filosofiche, religiose o sindacali e si riferisca a interessati che sono in contatto con i ridetti soggetti giuridici;
e) riguarda dati personali che sono stati resi manifestamente pubblici dall'interessato (ad esempio pubblicati su Facebook);
f) **è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali**. Questo vuole dire che **l'avvocato non ha necessità di acquisire il consenso preventivo per l'espletamento del mandato giudiziale**;
g) interesse pubblico rilevante proporzionato alla finalità perseguita. Non viene fornita alcuna indicazione in merito alla proporzione per cui ci si dovrà rimettere a un prudente apprezzamento;
h) è necessario per finalità di medicina preventiva o medicina del lavoro, assistenza o terapia sanitaria o sociale o gestione dei sistemi e dei servizi sanitari;
i) è necessario per motivi di interesse pubblico nel settore della sanità pubblica;
j) è necessario per motivi di archiviazione di pubblico interesse, di ricerca scientifica o storica o per fini statistici;
k) il titolare, il rappresentante, il responsabile o l'incaricato sono tenuti al segreto professionale.

I dati derivanti da **CONDANNE PENALI** o da **REATI** possono essere trattati SOLTANTO sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri.

4. Trattamento e finalità

Si definisce **TRATTAMENTO** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali (art. 4 n. 2).

A titolo esemplificativo, è Trattamento sia la mera raccolta e conservazione del dato sia la sua distruzione, passando per la consultazione e la comunicazione a terzi.

Il Trattamento deve essere lecito, corretto e trasparente (art. 5)

La **FINALITÀ** del trattamento è la ragione (giuridica) sottesa al trattamento.

A titolo esemplificativo, la finalità del trattamento può derivare da:

a) un adempimento contrattuale (ivi compreso il contratto di lavoro);
b) un obbligo legale;
c) un interesse vitale;
d) un interesse pubblico connesso a un pubblico potere;
e) un legittimo interesse prevalente.

Per cui, in uno studio legale, tra le finalità del trattamento potremo avere, ad esempio: gestione del contenzioso; pratiche stragiudiziali; gestione fornitori; gestione clienti; contabilità; gestione crediti; marketing; antiriciclaggio; interazione con i social network; interazione col sito web dello studio; comunicazioni commerciali; amministrazione del personale; gestione del personale; gestione di assicurazione sanitaria per dipendenti e collaboratori; assicurazione danni a terzi; gestione Legge 81/2008 Sicurezza sul lavoro; e così via

5. I Soggetti

Il Regolamento si preoccupa di definire i soggetti coinvolti dal trattamento dei dati personali.

Abbiamo già visto che INTERESSATO è la persona fisica individuata o individuabile attraverso il dato personale

5.1 Titolare

Titolare è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altro, determina le finalità e i mezzi del Trattamento.

5.1.1 Accountability (24)

In base al principio di **ACCOUNTABILITY**, traducibile con responsabilizzazione (art. 5 par. 2), il Titolare mette in atto misure tecniche e organizzative **adeguate** al fine di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.

Il concetto di adeguatezza non è definito nel regolamento (né altrove). Al fine della creazione di un'idea uniforme di tale concetto è auspicabile che trovino presto attuazione i codici di condotta e le certificazioni di cui agli artt. 40-43 del regolamento.

Nel frattempo, seppur vengono abrogate le misure minime quali quelle previste dell'allegato b del d.lgs. 196/2003, nulla vieta di utilizzarle come linee guida al fine di mettere in atto le misure adeguate.

5.1.2 Privacy by Design e Privacy By Default (25)

Il regolamento detta anche un principio generale che possa consentire al Titolare di "rendere il conto" (dimostrare) ai sensi dell'accountability: egli dovrà mettere in atto le ridette misure sia al momento di determinare i mezzi con cui il trattamento verrà effettuato sia al momento del trattamento stesso e si impegna a utilizzare soli i dati necessari per ogni specifica finalità.

In pratica e in altre parole qualora l'Avvocato abbia intenzione di raccogliere i dati in un archivio elettronico si preoccuperà innanzitutto di rendere quell'archivio il più sicuro possibile anche nei modi che verranno descritti più oltre (firewall, antivirus, … se si tratta di un archivio privato; nomina a responsabile del gestore del servizio cloud se si archivierà su un cloud; …). Secondo poi, al momento dell'acquisizione del dato, si preoccuperà di anonimizzarlo ad esempio, inserendolo in cartella che nominerà diversamente dal suo contenuto o altri accorgimenti simili o, meglio ancora, proteggendo le cartelle con una password.

Qualora, invece, raccolga i dati **anche** in forma cartacea dovrà procurarsi classificatori e cassetti provvisti di chiavi, possibilmente ignifughi, meglio ancora se certificati, e dovrà riporre e chiudere a chiave i dati (*rectius*, i documenti dove sono contenuti i dati) ogni qualvolta non siano soggetti al trattamento.

Il regolamento impone infatti di non rendere accessibili i dati a un numero indeterminato di persone.

5.2 Contitolare (26)

Sono **CONTITOLARI** coloro che concorrono a determinare le finalità e i mezzi del trattamento. I contitolari devono determinare in modo trasparente le rispettive responsabilità.

Esempi classici nello Studio legale sono quello dell'Associazione Professionale, fatti salvi diversi accordi interni, oppure il mandato congiunto. Può essere considerato come Contitolare anche il Consulente di Parte quando concorre a determinare finalità e mezzi del trattamento.

5.3 Rappresentante (27)

Qualora il Titolare o il Responsabile (vedi par. 5.4) abbiano sede fuori dall'Unione dovranno nominare un **RAPPRESENTANTE** (persona fisica o giuridica) che abbia lo stabilimento in uno degli Stati membri e che garantisca la conformità al regolamento.

5.4 Responsabile (28)

Il Regolamento definisce **RESPONSABILE** quel soggetto (persona fisica, giuridica, autorità pubblica, servizio o altro organismo) che tratta i dati **per conto** del Titolare.

Da questa breve definizione emerge che il Responsabile di cui parla il regolamento non è più quello ex art. 30 d.lgs. 196/2003, ma è un soggetto esterno cui il Titolare affida il trattamento di particolari categorie di dati e per determinate finalità.

A tal fine il titolare potrà rivolgersi solo a soggetti che, a loro volta, rispettino – mettendo in atto misure tecniche e organizzative adeguate – il Regolamento e siano in grado di dimostrarlo.

Tra il Titolare e il responsabile deve intercorrere un contratto/accordo scritto che sia vincolante per il Responsabile e che deve espressamente disciplinare come minimo:

a) la materia disciplinata;
b) la durata del trattamento;
c) la natura e la finalità del trattamento (è il Titolare che decide la finalità);
d) il tipo di dati personali (se particolari o meno. Ciò ai fini del consenso e delle altre esimenti al trattamento);
e) le categorie degli interessati;
f) gli obblighi e i diritti del Titolare del trattamento.

Sarà il Titolare a dover istruire il Responsabile sulla finalità per cui gli consente di trattare i dati per suo conto. Il Responsabile dovrà garantire per se stesso e per i suoi incaricati (vedi par. 5.5) di:

1 impegnarsi a un obbligo di riservatezza o averlo per legge;
2 aver adottato tutte le misure di sicurezza ai sensi dell'art. 32 del Regolamento (vedi par. 10);
3 quando intende ricorrere a sua volta ad un altro Responsabile lo faccia su autorizzazione del Titolare e si preoccupi di stipulare col nuovo Responsabile un contratto che abbia le stesse garanzie di quello che lo lega al Titolare;
4 aver adottato le misure tecniche e organizzative adeguate al trattamento che dovrà compiere;
5 assistere il Titolare al fine di garantire il rispetto di quanto previsto dalle norme sulla sicurezza dei dati personali (vedi par. 10);
6 impegnarsi a cancellare o restituire tutti i dati una volta raggiunta la finalità se è il Titolare a richiederlo;
7 impegnarsi ad essere collaborativo per ogni attività ispettiva e di revisione a carico o per conto del Titolare.

In pratica e in altre parole, anche il Responsabile dovrà garantire il rispetto del principio di Accountability previsto dall'art. 24, anche perché non bisogna dimenticare che il Responsabile è comunque un Titolare pro domo sua.

Il Responsabile che aderisse, nel momento in cui verranno ad esistenza, ai codici di condotta o alle certificazioni di cui agli artt. 40-42, avrà un sufficiente grado di affidabilità per quanto concerne il rispetto del Regolamento.

L'RGDP si preoccupa di specificare che il contratto tra Titolare e Responsabile potrà anche essere stipulato attraverso clausole tipo che verranno adottate dalla Commissione o dall'Autorità di Controllo (al momento non esistono).

Il regolamento dedica ben tre pagine al Responsabile, ma ciò nonostante molte parti sono lasciate alla libera interpretazione, la qual cosa sta creando diversi problemi interpretativi.

In particolare, non è ancora ben chiaro se debba essere nominato Responsabile il Commercialista, mentre nessun dubbio può sorgere in merito al Consulente del Lavoro o al Medico del Lavoro, così come nessun dubbio può sorgere in merito al provider di servizi web per quegli studi che abbiano un sito, un dominio

mail dedicato o comunque uno spazio hosting. Così come va assolutamente nominato Responsabile il provider di servizi cloud qualora ci sia, nonché la società fornitrice del Gestionale di studio.

Altra figura che si presenta ambigua rispetto alla nomina a Responsabile è il Domiciliatario o il sostituto d'udienza. Se questi avranno l'incarico di sostituire l'avvocato per meri adempimenti, quali la richiesta di un rinvio o la presenza a un'udienza che già si sa verrà rinviata, non avranno bisogno di alcuna nomina. Se però il domiciliatario o il sostituto d'udienza avranno anche il compito di discutere la causa potrebbe essere necessaria la nomina a Responsabile, con quanto ne consegue.

Nelle ultime settimane sono fioccate nomine da parte delle banche che hanno ritenuto di dover nominare Responsabili gli avvocati che si occupano, per loro conto, del recupero crediti. Il dibattito è aperto.

La figura del Responsabile rappresenta una delle opportunità per noi avvocati in quanto come abbiamo visto è una figura che, fra le altre cose, necessita di un contratto completo e complesso e che comporta delle responsabilità che solo un legale è in grado di affrontare al meglio.

5.5 L'incaricato (29)

Possono esistere dei soggetti, internamente alla struttura – nel nostro caso dello studio legale – cui il Titolare abbia autorizzato il trattamento dei dati.

Tali soggetti sono ad esempio i collaboratori, i praticanti, le segretarie/i segretari.

Il Regolamento si preoccupa di dire che tali soggetti possono trattare i dati SOLO se sono istruiti in tal senso dal Titolare. Non sono previste forme particolari di nomina/indicazione ma sarebbe opportuno anche in questo caso prevedere una forma scritta – anche l'aggiunta di semplici clausole al contratto di lavoro nel caso di segretarie/segretari ad esempio – anche al fine di garantire il Titolare nei casi di visite ispettive. Dovrebbe come minimo essere garantito, tra il Titolare e i suoi incaricati, un obbligo di riservatezza da parte di questi ultimi nonché l'obbligo di attenersi alle istruzioni.

5.6 Il Destinatario (4, n. 9)

Il **DESTINATARIO** è quel soggetto, persona fisica o giuridica, autorità pubblica, servizio o altro organismo che riceve comunicazione dei dati personali.

Per un avvocato/studio legale sono ad esempio destinatari: magistratura ed uffici giudiziari; camere di conciliazione e mediazione obbligatorie e non; colleghi per adempimenti obblighi di legge o di mandato; collaboratori (fatti salvi i casi in cui non siano incaricati del trattamento, vedi par. 5.5); corrispondenti; domiciliatari (fatti salvi in cui non siano Responsabili, vedi par. 5.4); commercialista (fatto salvo quanto detto al paragrafo 5.4); P.A. enti e società per adempimento incarico ricevuto; controparti per l'espletamento dell'incarico ricevuto; altri professionisti per l'espletamento dell'incarico ricevuto; Ordine degli Avvocati; Organismi di sovraindebitamento; Arbitri e Collegi Arbitrali; Service provider per posta elettronica e internet (quelli di terzi, non il nostro)

5.7 L'amministratore di sistema

La figura dell'**AMMINISTRATORE DI SISTEMA** è definita dalla l. 318/1999.

L'Amministratore di sistema è quel "*soggetto al quale è conferito il compito di sovraintendere alle risorse del sistema operativo di un elaboratore o di un sistema di una banca dati e di consentirne l'utilizzazione*".

Il Regolamento non nomina espressamente questa figura ma è facilmente intuibile che sia ancora presente e necessaria anche col nuovo impianto normativo.

Non lasciamoci ingannare dal fatto che questa figura sia stata normativamente prevista per grandi strutture al fine di garantire l'adeguato funzionamento del sistema informatico: nel piccolo studio legale l'Amministratore di sistema è identificabile col c.d. "tecnico del computer".

Tale soggetto, non rientrante in nessuna delle categorie sopraelencate, non tratta i dati (non li consulta neanche) se non per avventura. Ad ogni buon conto, per eccesso di zelo, sarà bene prevedere garanzie adeguate in tal senso anche tra il Titolare/Avvocato e l'Amministratore di sistema nelle forme che si riterranno più opportune sempre tenendo presente il principio dell'Accountability che mi impone fra l'altro, di "*rendere il conto*".

Attenzione a non nominarlo Responsabile, perché l'Amministratore di Sistema non tratta e non deve trattare i dati per conto del Titolare.

6. Le informative (12)

Il Regolamento ha modificato in modo importante l'informativa che deve essere data all'interessato. Anzi, LE informative.

Innanzitutto, l'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile. Nella sua redazione occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee.

Deve essere data, in linea di principio, per iscritto e preferibilmente in formato elettronico.

6.1 Ottenuti presso l'interessato (13)

Quando i dati vengono raccolti presso l'interessato l'informativa viene data nel momento stesso in cui dati vengono conferiti. Essa deve contenere **TASSATIVAMENTE**:

a) i dati di contatto del titolare del trattamento e di eventuali responsabili del trattamento;
b) i dati di contatto del responsabile della protezione dei dati, ove presente;
c) le finalità del trattamento cui sono destinati dati personali nonché la base giuridica del trattamento;
d) eventuali destinatari dei dati personali;
e) il periodo di conservazione dei dati;
f) l'esistenza del diritto di accesso rettifica o cancellazione, oltre al diritto alla portabilità dei dati;
g) l'esistenza del diritto di revocare il consenso in qualsiasi momento;
h) il diritto di proporre reclamo a un'autorità di controllo;
i) se il conferimento dei dati derivi da obbligo legale contrattuale;
j) l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

In pratica, l'informativa resa ai sensi dell'art. 13 è la sola che sarà resa dall'avvocato nello svolgimento del mandato professionale. Infatti, i dati dell'interessato possono essere comunicati soltanto e direttamente dallo stesso, dal suo rappresentante legale, curatore o tutore.

Sono fatti salvi casi particolari (ad esempio nel rapporto con le assicurazioni) ancora all'esame.

Per quanto riguarda il periodo di conservazione dei dati, per l'avvocato, possiamo individuare tre macro aree alternative fra loro:

- trascorsi 10 anni dal trattamento, o il maggior periodo necessario alla prescrizione dei diritti degli interessati e di terzi, derivanti dal loro trattamento;
- trascorsi i termini di legge per la loro conservazione a fini di archiviazione obbligatoria;
- trascorsi i termini per garantire il prosieguo dell'assistenza a detenuti e a persone scomparse e loro eredi.

Non è escluso che si possano individuare altri e diversi termini di conservazione dei dati.

È bene ricordare che qualora il titolare del trattamento/avvocato intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, deve fornire all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente fra quelle elencate.

L'informativa (o anche il semplice riferimento alla stessa) **NON VA INSERITA NEL MANDATO E NON È NECESSARIO FARLA SOTTOSCRIVERE AL CLIENTE**. Sarà sufficiente metterla in un luogo ben visibile (ad esempio sala d'attesa e scrivania personale) e attenzionare i clienti sulla stessa.

6.2 Ottenuti presso terzi (14)

Qualora i dati personali non siano stati ottenuti presso l'interessato, nell'informativa, oltre a quanto fin qui detto, dovrà essere indicata la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengono da fonti accessibili al pubblico.

Le informazioni dovranno essere fornite all'interessato entro un termine ragionevole, ma al più tardi entro un mese. Nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione con l'interessato. Nel caso sia prevista la comunicazione ad un altro destinatario, non oltre la prima comunicazione dei dati personali.

7. Il Consenso

Laddove uno studio legale intenda trattare dati personali per finalità non rientranti nell'esecuzione del contratto di prestazione d'opera professionale o per l'adempimento di obblighi legali, sarà necessario, al fine di soddisfare la condizione della liceità del trattamento, raccogliere l'espresso **CONSENSO** dell'interessato (art. 6 par. 1, lett. a).

Particolare è l'abbassamento dell'età dei minori ai fini del consenso che ora è di 16 anni, anche se i singoli Stati membri possono stabilirne di più basse.

Tale consenso deve essere liberamente prestato ed espresso previa una adeguata informativa (vedi par. 6) e deve essere inequivocabile.

Pertanto, anche se non espressamente previsto, qualora richiesto ai fini del trattamento sarà il caso che il Consenso venga espresso in forma scritta.

8. I diritti dell'interessato

Il Regolamento gravita attorno ai diritti dell'interessato cui è dedicato l'intero capo III (artt. 12-23)

8.1 Diritto d'accesso (15)

L'interessato che ne faccia richiesta ha sempre diritto di ottenere una copia dei propri dati oggetto di trattamento.

Potrà inoltre conoscere le finalità del trattamento, ma il titolare non è tenuto a comunicare le modalità del trattamento.

Sarà necessario indicare il periodo di conservazione dei dati o i criteri utilizzati per determinare tale periodo.

L'interessato ha anche diritto ad ottenere la rettifica o l'integrazione dei dati che lo riguardano.

8.2 Diritto all'oblio (17)

Il diritto all'oblio è diritto ad ottenere la cancellazione dei propri dati.

Tale diritto può essere ottenuto:

a) se i dati personali non sono necessari rispetto alle finalità;
b) se intervenuta revoca del consenso e non esiste altro fondamento giuridico per il trattamento;
c) se i dati sono trattati illecitamente;
d) se, a certe condizioni e in ipotesi specifiche, l'interessato si oppone al trattamento;
e) se è necessario cancellarli per adempiere un obbligo legale;

f) se sono stati raccolti relativamente all'offerta di servizi della società dell'informazione nei confronti di soggetti minori di anni 16.

Se il titolare ha reso pubblici i dati oggetto di trattamento e l'interessato abbia fatto richiesta di cancellazione è fatto obbligo di informare i titolari del trattamento che stanno trattando i medesimi dati, salvo il caso di diritto alla libertà di espressione e di informazione e di adempimento di un obbligo legale.

8.3 Limitazione di trattamento (18)

Consiste nella possibilità da parte dell'interessato di limitare in tutto o in parte il trattamento e di impedire al titolare la cancellazione dei propri dati quando vi abbia interesse. L'interesse potrebbe derivare, ad esempio, dal diritto alla portabilità (vedi par. 8.4)

Può essere richiesto:

a) quando l'interessato contesta l'esattezza dei dati personali;
b) quando il trattamento è illecito e l'interessato si oppone alla cancellazione e chiede invece che ne sia limitato l'utilizzo;
c) benché il titolare non abbia più bisogno di trattamento ma i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) se è stata fatta opposizione ai fini di verificare l'eventuale prevalenza di motivi legittimi da parte del titolare

8.4 Diritto alla portabilità (20)

Si applica solo ai trattamenti automatizzati.

Sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato.

Sono portabili solo i dati che siano stati "forniti" dall'interessato al titolare

L'interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano e al diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti.

Un esempio è quello della portabilità del numero telefonico.

8.5 Diritto di opposizione (21)

L'interessato, qualora sussistano motivi legittimi, ha diritto di opporsi in qualsiasi momento al trattamento. In caso di opposizione il titolare potrà continuare a trattare i dati solo in caso dimostri un legittimo interesse prevalente.

9. Il Registro (30)

È un **REGISTRO** delle attività di trattamento svolte sotto la responsabilità del titolare. È obbligatorio per ogni titolare. Ricorda un po' il vecchio DPS (Documento Programmatico sulla Sicurezza)

Deve contenere:

a) il nome dei dati di contatto del titolare, del rappresentante del titolare e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie dei destinatari a cui i dati sono stati e saranno comunicati, compresi i destinatari di paesi terzi o organizzazioni internazionali;
e) qualora i dati vengano effettivamente trasferiti verso paesi terzi l'indicazione di tali paesi, nonché la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure tecniche e organizzative per la sicurezza dei dati.

Qualora il trattamento venga effettuato da un responsabile del trattamento o da un rappresentante e quel trattamento rientri tra quelli soggetti a Registro dei trattamenti questi saranno tenuti a tenere il registro con le medesime caratteristiche di cui sopra.

È possibile nominare un responsabile del trattamento solo per alcune categorie di dati pertanto egli dovrà tenere un registro relativo solo ai dati effettivamente trattati

I registri sono tenuti in forma scritta anche in formato elettronico e su richiesta devono essere messi a disposizione dell'autorità di controllo.

L'obbligo della tenuta del registro è sancito dal regolamento solo per le imprese e organizzazioni con 250 dipendenti e oltre, salvo che il trattamento non presenti rischio per i diritti e le libertà dell'interessato, il trattamento **non sia occasionale o includa trattamento di categorie particolari di dati (ex sensibili) o dati personali relativi a condanne penali per reati**.

Dato l'ultimo inciso, nonostante non sia sancito un obbligo specifico per gli avvocati, ben si comprende come i dati trattati facilmente potrebbero ricadere tra quelli che rendono il Registro obbligatorio. Pertanto, la tenuta del Registro è fortemente consigliata.

D'altronde il WP 29 (Gruppo di lavoro art. 29, formato dalle Autorità di tutti gli Stati membri UE) ha sottolineato che le tre tipologie di trattamento sono alternative e la presenza di una sola di queste determina l'obbligo di redazione del registro. Inoltre, ha specificato che per "*rischio per i diritti e le libertà dell'interessato*" non deve intendersi "*alto rischio*".

Si aggiunga poi che il Garante l'ha consigliata in modo generico a tutti i titolari.

Un'ultima osservazione: la normativa non prevede che il documento così formato debba avere una data certa. Ad ogni buon conto, per il formato tenuto elettronicamente, a fini probatori, il registro può essere firmato digitalmente e inviato via pec a se stessi, oppure dopo averlo firmato digitalmente gli si può applicare una marca temporale.

10. La sicurezza: il Data Breach (32)

La **VIOLAZIONE DI SICUREZZA** che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non automatizzata o l'accesso ai dati personali trasmessi conservati o comunque trattati (4, n. 12)

Le misure di sicurezza devono garantire un livello di sicurezza adeguato al rischio.

Nel regolamento non si parla più di misure minime di sicurezza. Considerato che spetta al titolare del trattamento stabilire quali sono le misure adeguate il consiglio è di tener sempre presente i "consigli" elencati dal d.lgs. 196/2003 in proposito e in particolare le misure elencate nell'allegato b) in quanto, almeno fino a quando non vedranno la luce i codici di condotta e gli schemi di certificazione di cui agli artt. 40-42, volti a garantire l'adeguatezza delle misure di sicurezza adottate, l'elenco menzionato può rappresentare un buon metro di adeguamento.

L'art. 32 contiene una lista aperta di misure di sicurezza. Fra queste:

a) La pseudominimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche organizzative al fine di garantire la sicurezza del trattamento.

In caso di violazione dei dati personali a seguito di attacco informatico o anche alterazione del dato, il titolare del trattamento **notifica tale violazione all'autorità garante** senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. (33)

Il Regolamento si preoccupa anche di indicare cosa deve contenere la notifica: descrivere la natura della violazione dei dati personali e le categorie e il numero approssimativo di interessati colpiti, nonché le categorie e il numero approssimativo di registrazione dei dati personali in questione; comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto; descrivere le probabili conseguenze della violazione; **descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione e per attenuare i possibili effetti negativi**.

Questo per due ordini di ragioni: la prima è che se il titolare avrà adottato le misure tecniche e organizzative adeguate ad evitare la violazione non sarà passibile di sanzione; la seconda è che se lo avrà fatto non dovrà neanche dare comunicazione della violazione all'interessato.

11. Le Sanzioni

Le **SANZIONI** per l'inosservanza del regolamento sono molto pesanti: fino a 10.000.000 di euro (o, per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente se superiore) in alcuni casi e in altri fino a **20.000.000,00** di **EURO** (o, per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore). Sebbene è pur vero che uno studio legale/medio piccolo difficilmente potrà arrivare a sanzioni di tale importo è bene conoscere a fondo tale possibilità soprattutto ai fini di, **cogliendo l'attimo**, consigliare al meglio la propria clientela.

12. Compliance Checklist per avvocati

Ricapitolando, questi sono i passi che uno studio legale di dimensioni medio/piccole dovrà eseguire al fine di essere *compliant*:

1. Individuare le tipologie di trattamento effettuate e i tipi di dati (comuni, particolari, penali). In particolare, se ci sono solo clienti o se si hanno dipendenti – segretaria/o – se ci si serve da fornitori per le strumentazioni e prodotti di cancelleria e così via.
2. Individuare eventuali soggetti autorizzati – incaricati interni – come ad esempio dipendenti e praticanti che hanno accesso ai dati anche solo per consultazione, che equivale a un trattamento.
3. Individuare se ci sono Responsabili del trattamento, come ad esempio il consulente del lavoro e il gestore dei servizi web (anche la mail professionale rientra tra i servizi web, **prestate attenzione a chi è il gestore e se accetta o meno la nomina a responsabile**)
4. Censire la parte fisica (classificatori, armadi, cassetti, misure antincendio e così via) e la parte informatica (quanti pc? Che Sistema Operativo? Quante reti? Che antivirus? Come sono le password? Fotocopiatori digitali in rete? Scanner digitali in rete? Dove sono i dati? In un singolo pc/hd? Su un server? In cloud? Ogni quanto si fa il backup? E così via).

All'esito di queste prime attività si sarà compiuta buona parte di quella che nel Regolamento viene definita Valutazione di impatto e sarà più semplice

5. Compilare il **Registro dei trattamenti** che, come abbiamo detto, anche se non obbligatorio è fortemente consigliato, anche perché non ci vuol molto a che diventi obbligatorio.
6. Revisionare tutta la documentazione già esistente, in particolare l'informativa. Si dovranno altresì stipulare i contratti con gli eventuali responsabili e prevedere di dare le adeguate istruzioni ai soggetti incaricati.

7. Individuare i rischi (informatico e ambientale) e le contromisure, quelle adottate e quelle da adottare. Implementare le procedure di Data Breach.
8. Predisporre la documentazione idonea ai fini di verifiche ispettive e per sicurezza personale (accountability).

NON RIGUARDA GLI STUDI LEGALI MEDIO/PICCOLI la nomina di un Responsabile per la Protezione Dati (DPO, vedi par. 14)

13. Le valutazioni di impatto (35, 36)

In caso di un rischio elevato per i diritti delle libertà delle persone fisiche prima di procedere al trattamento si deve effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

La valutazione è obbligatoria quando si esegue:

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

La valutazione deve contenere almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso l'interesse legittimo perseguito dal titolare del trattamento ove esistente;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;

Nella valutazione dovranno anche essere indicate le misure per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti, degli interessi legittimi degli interessati e delle altre persone in questione.

Si intuisce che la valutazione di impatto, il cui esito potrebbe anche comportare una consultazione con l'Autorità al fine di valutare l'opportunità del trattamento (art. 36), è un meccanismo complesso e andrà effettuata per ogni distinto trattamento attuato/da attuare. Tale adempimento non sempre – quasi mai – è necessario per lo studio legale/medio piccolo.

Essa, però, rappresenta comunque un'altra opportunità per l'avvocato, in quanto per la sua compilazione sarà necessaria la presenza di un legale eventualmente affiancato da un tecnico informatico.

14. Il Data Protection Officer (37-39)

Il **DPO** è una figura finalizzata a facilitare l'attuazione del regolamento da parte del titolare/responsabile.

Fra i compiti del RPD (Responsabile Protezione Dati) rientra "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto (ma anche semplicemente del Data Protection Assessment)

Il titolare del trattamento ha l'obbligo di nominare il responsabile per la protezione dei dati se è:

a) un soggetto pubblico;
b) un soggetto pubblico o privato che come attività principale svolge attività implicanti monitoraggio regolare e sistematico di interessi su larga scala;
c) un soggetto pubblico o privato che come attività principale svolge attività implicanti trattamenti di dati particolari e/o dati giudiziari su larga scala.

Il fatto che non sia prevista un'obbligatorietà incondizionata per la nomina del DPO non esclude che, in particolar modo nelle imprese medio/grandi, questa figura sia fortemente consigliata soprattutto per agevolare il titolare nel rispetto del principio dell'accountability. Rispetto che, qualora il titolare operasse da solo, potrebbe risultare diabolico.

Infatti, con un'elencazione aperta, i compiti del DPO possono così riassumersi:

1. informare e fornire consulenza in merito agli obblighi derivanti dal regolamento;
2. sorvegliare l'osservanza del regolamento e delle altre disposizioni normative in materia di protezione dei dati personali;
3. fornire parere sulla valutazione di impatto;
4. cooperare con l'autorità di controllo;
5. fungere da punto di contatto dell'autorità di controllo per questioni connesse al trattamento;
6. avere approccio basato sul rischio;
7. e così via.

Il DPO deve essere tempestivamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali fin dalle fasi iniziali; deve essere: indipendente, autorevole e avere competenze e conoscenze specifiche della materia.

La nomina andrà comunicata:

- all'Autorità Garante, mediante modulo messo a disposizione dall'autorità stessa;
- a tutto il personale (non solo a chi tratta i dati);
- al/ai responsabile del trattamento;
- come già detto i dati di contatto del DPO andranno inseriti nell'informativa.

Come ben si comprende il DPO, che non rappresenta – ancora – una professione regolamentata, è una figura altamente professionale, con compiti che, senza timore, possono descriversi come manageriali e che deve possedere competenze e caratteristiche altamente qualificate.

A scanso di equivoci, **la nomina del DPO può dirsi esclusa con un certo grado di certezza per gli studi legali medio/piccoli.**

Il Data Protection Officer rappresenta, dunque, un'ulteriore opportunità per il professionista avvocato. (vedi anche norma UNI 11697/2017, **Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza**)

15. Il Trasferimento dei Dati all'Estero (Capo V, 44-50)

Il Capo V del GDPR espressamente regola l'ipotesi di trasferimento dei dati personali all'estero, intendendosi per estero gli Stati che non appartengono allo Spazio Economico Europeo. Il principio generale posto dal Regolamento è che il trasferimento è consentito solo se avviene in conformità al Capo V medesimo, nonché a tutte le altre previsioni del GDPR.

ATTENZIONE: questo significa che, se ci si rivolge a servizi esteri (ad es., Google Frive, Dpopbox, Amazon Cloud, Yahoo mail, Gmail, Outlook, etc), bisogna verificare le condizioni di utilizzo. Se queste non garantiscono standard di sicurezza e continuità del servizio elevati, si rischia di incorrere in violazioni di altri Capi del Regolamento: **ad esempio, se l'account può essere chiuso in qualsiasi momento, non è possibile garantire i diritti dell'interessato**.

È possibile trasferire i dati all'Estero se (alternativamente):

a) esiste una decisione di adeguatezza della Commissione Europea, ossia un provvedimento – come il c.d. Privacy Shield – con cui la Commissione individua dei Paesi che assicurano dei livelli minimi di rispetto della privacy;

b) se sono adottate le cc.dd. "garanzie adeguate": si tratta, *in primis*, delle clausole contrattuali standard o delle Norme vincolanti di impresa, ipotesi più confacenti alle imprese che non agli avvocati. Altre garanzie adeguate sono, poi, l'impegno a rispettare un codice di condotta approvato o un meccanismo di certificazione (artt. 40-43, vedi par. 5.1.1)
c) in mancanza anche delle garanzie adeguate, il trasferimento è possibile solo se vi sono esplicite deroghe, tra cui le più importanti sono:

- esplicito consenso dell'interessato, informato preventivamente dei possibili rischi dovuti alla mancanza di decisioni di adeguatezza e di garanzie adeguate;
- se il trattamento è necessario all'esecuzione di misure contrattuali (non s'intende il contratto tra cliente e avvocato);
- se il trattamento è necessario per accertare un diritto in sede giudiziaria (es., rogatoria internazionale);
- se i dati sono tratti da un registro di pubblica conoscibilità, purché siano rispettate le condizioni di accesso al registro a norma del diritto interno o dellìUnione (ma deve pur sempre sussistere una valida ragione per trasferire i dati all'estero).

Infine, si deve rilevare che la disciplina del trasferimento dei dati all'estero è soggetta a numerose limitazioni, per cui si consiglia di leggere con attenzione il Capo V del Regolamento e di non ricorrere, per quanto più possibile, a servizi collocati extra-UE.

16. Qualche cenno sui mezzi di ricorso (Capo VIII, 77-84)

Qualora l'interessato ritenga che il trattamento che lo riguardi abbia violato il Regolamento ha diritto a proporre reclamo a un'autorità di controllo, segnatamente **nello Stato membro in cui risiede o lavora abitualmente o del luogo ove si è verificata la presunta violazione**, fatto salvo ogni altro ricorso giurisdizionale o amministrativo.

Chiunque subisca un danno causato da una violazione del Regolamento ha diritto ad ottenere il risarcimento dal Titolare o dal Responsabile. Le azioni si propongono a norma del diritto dello Stato membro del Titolare e/o del Responsabile o, in alternativa, di quello ove l'interessato risiede.

17. Fonti normative, strumenti, informazioni di contatto e ringraziamenti

Trattato sull'Unione Europea: https://tinyurl.com/yarze8vn
Decreto Legislativo 196/2003 (Codice Privacy): https://tinyurl.com/y8628sya
Allegato B. Misure minime di sicurezza: https://tinyurl.com/ycm3yyuu
Regolamento Europeo 679/2016 con "Considerando": https://tinyurl.com/yaw3mg88

Modello Informativa Studio Legale
Modello di Registro delle attività di Trattamento Studio Legale

Nella speranza di aver fatto cosa gradita ai colleghi
Commissione Informatica del Consiglio dell'Ordine degli Avvocati di Bari
www.ordineavvocati.bari.it
mail: commissioneinformatica.coabari@gmail.com

Si ringrazia l'Avv. Francesco Minazzi, foro de L'Aquila, per il *Capitolo 15, Trasferimento dei dati all'Estero.*

Si ringrazia l'Avv. Fabrizio Sigillò, foro di Catanzaro, per il prezioso aiuto nella formattazione dell'*Informativa.*