FAQ

PRIVACY E STUDI LEGALI

a cura della Commissione *"Privacy"* dell'Ordine degli Avvocati di Roma

* * * *

1. – INTRODUZIONE

(a cura dell'Avv. Gianluca DI ASCENZO)

Il 25 Maggio 2018 è divenuto definitivamente applicabile negli Stati membri il Regolamento UE n. 2016/679, Regolamento generale sulla protezione dei dati, noto a tutti con l'acronimo inglese GDPR (*General Data Protection Regulation*), che stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Le Istituzioni forensi si sono attivate per chiarire l'impatto di tale normativa nell'esercizio della professione forense, elaborando vademecum e Linee Guida: una tra tutte, *"Il GDPR e l'Avvocato"*, a cura del Consiglio Nazionale Forense (1).

Nel mese di Agosto 2018, poi, il quadro della disciplina in materia di *privacy* si è integrato con l'approvazione del d.lgs. 10/08/2018, n. 101, recante: *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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)*(2).

Il d.lgs. n. 101/2018 ha introdotto modifiche al Codice in materia di protezione dei dati personali di cui al d.lgs. 30/06/2003, n. 196 per adeguarlo al GDPR; ha disciplinato, ad es., la previsione di fattispecie penali, le misure per la tutela in via amministrativa o giudiziale alle controversie in materia di protezione dei dati personali, le regole deontologiche che hanno sostituito i Codici di deontologia e di buona condotta per i trattamenti di dati personali.

Il panorama normativo, poi, si è arricchito ulteriormente con l'approvazione delle *"Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del*

---

(1) *https://www.consiglionazionaleforense.it/documents/20182/445621/IL+GDPR+E+L%27AVVOCATO/ef231b75-2066-43df-8d88-570bf0ea98b3*

(2) *https://www.gpdp.it/home/ricerca/-/search/tipologia/Normativa%20italiana; https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29*

d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018" ([3]), (Pubblicato sulla Gazzetta Ufficiale n. 12 del 15 gennaio 2019).

Tali regole deontologiche, come si legge nell'art. 1 del citato provvedimento, *"devono essere rispettate nel trattamento di dati personali per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, sia nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, sia nella fase successiva alla sua definizione, da parte di: a) avvocati o praticanti avvocati iscritti ad albi territoriali o ai relativi registri, sezioni ed elenchi, i quali esercitino l'attività in forma individuale, associata o societaria svolgendo, anche su mandato, un'attività in sede giurisdizionale o di consulenza o di assistenza stragiudiziale, anche avvalendosi di collaboratori, dipendenti o ausiliari, nonché da avvocati stranieri esercenti legalmente la professione sul territorio dello Stato; b) soggetti che, sulla base di uno specifico incarico anche da parte di un difensore, svolgano in conformità alla legge attività di investigazione privata (art. 134 r.d. 18 giugno 1931, n. 773; art. 222 norme di coordinamento del c.p.p.). [...] si applicano, altresì, a chiunque tratti dati personali per le finalità di cui al comma 1, in particolare a altri liberi professionisti o soggetti che in conformità alla legge prestino, su mandato, attività di assistenza o consulenza per le medesime finalità."*

Per quanto riguarda il trattamento dei dati da parte di avvocati, l'art. 2) disciplina le modalità di trattamento; l'art. 3) l'informativa unica; l'art. 4) la conservazione e cancellazione dei dati; l'art. 5) la comunicazione e diffusione di dati; l'art. 6) gli accertamenti riguardanti la documentazione detenuta dal difensore.

Ciò brevemente premesso, la presente iniziativa, a cura della Commissione *ex* art. 32, L. 247/2012 *"Privacy"* dell'Ordine degli Avvocati di Roma, fa seguito alle attività seminariali organizzate nel corso degli anni 2018 e 2019, in particolare agli eventi *"La privacy negli studi legali: il GDPR in pillole"* del 10/12/2018 e *"La privacy negli studi legali 2.0"* del 09/10/2019.

Questa pubblicazione, lungi dall'avere la pretesa dell'esaustività, con mero spirito collaborativo, intende fornire uno strumento agile per gli Avvocati, nell'ottica di offrire indicazioni operative utili nello svolgimento quotidiano della professione forense.

Il vademecum, in particolare, è stato elaborato sotto forma di *"F.A.Q."* — acronimo di *"Frequently Asked Questions"*, ossia risposte alle domande più frequenti — a mero scopo informativo, per offrire un contributo agli Avvocati, nel rispetto dei principi richiamati nel GDPR, nella Carta dei Diritti fondamentali dell'Unione Europea e nel Trattato sul

[3]https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069653

Funzionamento dell'Unione Europea, ovvero che ogni persona ha diritto alla protezione dei dati di carattere personale che la concernono.

Si cercherà, pertanto, di richiamare l'attenzione, tra gli altri, sui doveri di trasparenza con la clientela; sulla gestione dei dati nei rapporti con dipendenti, collaboratori di studio, corrispondenti e domiciliatari; sull'adozione di una *"privacy policy"* dell'Avvocato, che tenga conto delle novità in materia di informativa e consenso, registro dei trattamenti, misure di sicurezza e *data breach;* sulla valutazione dei rischi e valutazione di impatto.

Tutto quanto precede in ottemperanza al principio di responsabilizzazione o *"accountability"*.

Il Garante per la Protezione dei Dati Personali ha, infatti, chiarito che:

"Il Regolamento pone con forza 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 assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del Regolamento). 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" (4).

* * * *

2. — I SOGGETTI PRIVACY

(a cura degli Avv.ti Jacopo DE PONTE, Claudia DI BERNARDINO e Maria Lilia LA PORTA)

D: Chi è il Titolare del Trattamento?

R: Ai sensi dell'art. 4, par. 1 n. 7) del GDPR 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"*.

Pertanto, con riferimento al trattamento dei dati svolto da un libero professionista, il titolare del trattamento sarà il singolo Avvocato.

D: Come si fa ad individuare il Titolare del trattamento?

R: Il titolare del trattamento è il soggetto che ha potere decisionale in ordine alle modalità e finalità del trattamento.

---

(4) *https://www.garanteprivacy.it/en/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili*

In concreto, si pensi al singolo Avvocato che, acquisiti i dati del cliente, decide autonomamente in che modo trattarli, come utilizzarli, gestirli e conservarli, per quali finalità e quali misure di sicurezza adottare per proteggere tale trattamento.

D: Chi è il titolare del trattamento in uno studio legale?

R: Nel caso di uno studio legale con singoli Avvocati, non in forma associata, il titolare del trattamento sarà il singolo avvocato con riferimento ai dati che il medesimo tratta.

In concreto, il singolo Avvocato sarà titolare del trattamento con riferimento ai dati dei propri assistiti.

D: Chi è il titolare del trattamento nel caso di studio associato o società tra professionisti?

R: Nel caso di uno studio legale associato o in forma societaria, il titolare del trattamento è la persona giuridica.

D: Cosa è la Contitolarità?

R: La Contitolarità, prevista dall'art. 26 GDPR, si verifica quando due o più titolari del trattamento condividono un trattamento di dati.

In tal caso, non sarà un solo avvocato ad avere il potere decisionale su un determinato trattamento, ma tale potere sarà condiviso con un collega.

È il classico esempio di un incarico condiviso. Il GDPR prevede che i due avvocati contitolari debbano stipulare un accordo interno di contitolarità, in cui specificare in modo espresso le rispettive attività, finalità e modalità di trattamento, nonché gli ambiti di competenza e responsabilità.

D: Chi è il Responsabile del trattamento?

R: Il Regolamento definisce (art. 4 par. 1, n. 8) che il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

D: Cosa fa in concreto il Responsabile del trattamento?

R: Il Responsabile del trattamento viene analiticamente disciplinato dal GDPR agli artt. 28 e seguenti, dai quali si ricava che, detta figura, è necessariamente presente ogniqualvolta il titolare del trattamento (e quindi, nel caso degli studi legali, l'avvocato e/o gli avvocati

titolari dello studio e/o le associazioni professionali) intenda delegare il trattamento dei dati personali.

Il responsabile deve presentare garanzie sufficienti a mettere in atto misure tecniche organizzative che rispettino i parametri richiesti dal Regolamento Europeo e al contempo garantiscano la piena e regolare tutela dei diritti dell'interessato.

D: Come deve essere nominato il Responsabile del trattamento?

R: L'art. 28 n. 3 del GDPR, prevede espressamente che i trattamenti dei dati effettuati dal responsabile del trattamento vengano contrattualizzati, in modo tale che il responsabile sia vincolato al titolare del trattamento e che vengano pattuiti ed enucleati la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento medesimo, il tipo di dati personali e le categorie di interessati e, infine, gli obblighi e i diritti del titolare del trattamento (si rimanda direttamente al testo di legge per gli altri e più specifici adempimenti previsti dalla norma).

D: Chi sono i Sub-Responsabili?

R: L'art. 28 introduce, altresì, la figura del *"Sub-Responsabile"*, ossia di un ulteriore soggetto responsabile del trattamento dei dati individuato dal responsabile del trattamento, previa autorizzazione scritta (specifica o generale a seconda dei casi) da parte del titolare del trattamento al subentro di altri, appunto, (sub) responsabili.

D: Quali sono i rapporti tra Responsabile del trattamento e Sub-Responsabili?

R: Nel caso in cui il responsabile del trattamento — scelto direttamente dal titolare del trattamento — abbia un'autorizzazione generale da parte del titolare stesso ad avvalersi di sub-responsabili, ripartendo così la propria responsabilità circa il trattamento dei dati, resta comunque salva la facoltà per il titolare di potersi opporre alle ulteriori designazioni effettuate.

In definitiva, il/i soggetti responsabili del trattamento, dovranno sempre informare il titolare in merito a ogni eventuale modifica dagli stessi apportata.

Gli obblighi e le prescrizioni di cui sopra (tra titolare e responsabile), sono imposti — sempre mediante contratto o altro atto equipollente secondo il diritto UE — anche ai Sub-Responsabili eventualmente individuati dal responsabile per l'esecuzione di specifiche attività di trattamento.

D: Chi sono i Responsabili del trattamento di uno studio legale?

R: All'interno di uno studio legale, poiché il GDPR individua il Responsabile del trattamento quale soggetto che tratta i dati personali per conto del titolare del trattamento (art. 4 n. 8), è verosimile che detta figura sia esterna al contesto professionale (e/o aziendale) e che sia quindi individuabile, a titolo esemplificativo ma non esaustivo, nella società di informatica e/o nel tecnico e/o professionista — anche non informatico — che gestisca il *server* dello studio legale e che, quindi, abbia costante accesso ai dati personali trattati e salvati dallo studio.

Una volta individuato il responsabile del trattamento, il titolare deve procedere a sottoporre allo stesso un accordo scritto nel quale vengono formalizzate le rispettive responsabilità, istruzioni ed adempimenti per il corretto trattamento dei dati del titolare del trattamento da parte del responsabile nominato.

D: Chi è l'Autorizzato al trattamento?

R: Il Regolamento, differentemente dal d.lgs. n. 196/2003, pur non prevedendo espressamente la figura dell'incaricato, non ne esclude la nomina, facendo riferimento a *"persone autorizzate"* al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4, par. 1, n. 10 GDPR).

L'Autorizzato, quindi, è il soggetto (persona fisica) che effettua materialmente le operazioni di trattamento sui dati personali. Ciò non esclude a priori che tale figura sia esterna allo studio o all'azienda, ma nella pratica è ipotesi difficilmente concretizzabile.

Gli autorizzati — che possono essere organizzati con diversi livelli di delega — possono operare alle dipendenze del titolare, ma anche del responsabile ove nominato.

Sebbene il Regolamento non preveda obblighi di nomina o di designazione formale per gli autorizzati, resta, tuttavia, fondamentale fornire agli autorizzati tutte le istruzioni operative (art. 29 GDPR), inclusi gli obblighi inerenti alle misure di sicurezza e che sia fornita loro la necessaria formazione.

La designazione degli autorizzati deve avvenire per iscritto e può avvenire anche con unico atto per più persone.

L'eventuale designazione non necessita di firma per accettazione, anche se è sempre consigliabile disporre di una firma che certifichi la presa visione dell'autorizzato in merito alle istruzioni impartitegli, cui lo stesso deve rigidamente attenersi e seguire.

D: Chi sono gli Autorizzati al trattamento all'interno di uno studio legale?

R:L'Autorizzato, in definitiva, è colui che materialmente compie il trattamento dei dati personali all'interno della struttura presso cui è inserito e, tanto più nel contesto di uno studio legale, tale figura può essere solamente una persona fisica che agisca sotto il controllo diretto del titolare del trattamento e/o del responsabile — e quindi dell'avvocato e/o dei professionisti di cui il titolare si avvale quali responsabili — e può essere individuato, a mero titolo esemplificativo ma non esaustivo, nel personale di segreteria, nei praticanti o, in generale, nei collaboratori di studio che non siano titolari del trattamento.

D: Chi è il DPO?

R: DPO (*Data Protection Officer*) o RPD (Responsabile della protezione dei dati) è una figura introdotta dall'art. 37 del GDPR. Viene definito come *"facilitatore"*, in quanto facilita l'osservanza della normativa in materia di protezione dei dati, partecipa alle attività del titolare del trattamento ed è un punto di contatto con l'autorità di controllo nazionale e con gli interessati.

A tal proposito, l'art. 39 del GDPR offre un elenco dei principali compiti del DPO.

Tale ruolo può essere rivestito da una persona fisica o da una persona giuridica e il titolare del trattamento può scegliere di nominare un DPO all'interno della propria struttura oppure di designare un DPO esterno.

La designazione deve avvenire in forma scritta, mediante atto di designazione e in caso di DPO esterno deve essere predisposto un contratto di servizi tra DPO nominando e titolare del trattamento.

I dati del DPO designato devono, poi, essere comunicati al Garante Privacy.

D: Che competenze deve avere il DPO?

R: Il DPO deve 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 di riferimento.

Nello svolgimento delle attività di sua competenza deve essere inoltre coinvolto, interessato e sostenuto dal titolare o dal responsabile del trattamento, che devono anche garantire la sua terzietà ed indipendenza (art. 38 del GDPR).

D: Quando deve essere designato il DPO?

R: Il titolare del trattamento deve obbligatoriamente nominare un DPO ove ricorra uno dei tre casi individuati dall'art. 37 par. 1 lett. a), b) e c) del GDPR, ossia se:

"a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10."

D: Quando deve essere designato il DPO in uno studio legale?

R: Per quanto riguarda uno studio legale, esclusa la rilevanza dell'ipotesi di cui alla lett. a) dell'art. 37 del GDPR, si deve far riferimento ai criteri indicati nella lettera c) e, quindi, valutare se l'attività dello studio legale consista in un trattamento su larga scala di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10.

D: Tutti gli studi legali devono nominare il DPO?

R: Come indicato dalle Linee Guida del WP sull'art. 29 ([5]), il singolo avvocato non ricade nell'ipotesi di obbligatorietà della nomina del DPO, in quanto è difficile che effettui trattamenti di categorie particolari di dati o di dati relativi a condanne penali o reati che possano essere ricompresi nel concetto di larga scala.

È, al contrario, altamente probabile che uno studio maggiormente strutturato o uno studio associato o in forma societaria effettui trattamenti su larga scala e ricada nell'obbligo di designazione del DPO.

Il parametro da tenere in considerazione è pertanto quello della *"larga scala"*.

Tuttavia, si tratta di indicazioni di massima e tale scelta deve essere valutata caso per caso.

D: È possibile una designazione volontaria del DPO?

([5]) *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048*

R: Sì, anche se lo studio legale non rientra in nessuna delle ipotesi di obbligatorietà della nomina del DPO, il titolare del trattamento può scegliere di procedere ad una designazione su base volontaria, seguendo le medesime norme previste in caso di nomina obbligatoria.

* * * *

3. — INFORMATIVA E CONSENSO

(a cura degli Avv.ti Gianmarco CENCI, Eugenio CIPOLLA, Maria Lilia LA PORTA, Antonietta MARESCHI e Carmela MARTUSCIELLO)

D: Cosa è l'informativa?

R: L'informativa è un documento contenente tutte le informazioni che il Titolare del trattamento è tenuto a fornire agli interessati in merito al trattamento dei loro dati.

D: Che caratteristiche deve avere l'informativa?

R: Il GDPR indica in modo molto più analitico rispetto al Codice Privacy le caratteristiche dell'informativa, disponendo che sia resa all'interessato in modo trasparente, conciso, intellegibile e facilmente accessibile, con linguaggio semplice e chiaro (così come indicato anche dalle Linee Guida del WP art. 29 sulla Trasparenza) (6).

D: Che cosa deve contenere l'informativa?

R: Gli artt. 13 e 14 del GDPR (cui si rimanda) distinguono l'ipotesi in cui i dati siano raccolti presso l'interessato (si pensi al singolo cliente che dà l'incarico all'Avvocato), da quelli in cui i dati siano forniti da terzi (si pensi al caso dei dati della controparte rispetto all'assistito o ancora dei dati ottenuti a seguito dell'affidamento da parte del Tribunale dell'incarico di difensore d'ufficio, curatore, custode e delegato alle vendite, ecc.) e indicano in modo specifico quali informazioni occorre fornire all'interessato.

In particolare, il GDPR prevede l'indicazione di alcuni nuovi elementi: dati di contatto del Titolare e del RPD-DPO, ove esistente, base giuridica del trattamento, eventuale interesse legittimo perseguito dal titolare, eventuale trasferimento di dati in Paesi terzi extra UE e, in caso affermativo, relativi strumenti, periodo di conservazione dei dati, diritto di presentare un reclamo all'autorità di controllo, eventuale presenza di processi decisionali automatizzati, inclusa la profilazione.

---

(6) *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227*

D: Quando deve essere fornita l'informativa all'interessato (in particolare al cliente)?

R: Nel caso di cui all'art. 13 del GDPR, ossia nell'ipotesi in cui i dati siano raccolti presso l'interessato, l'informativa deve essere fornita nel momento in cui vengono acquisiti i dati.

Ai sensi dell'art. 3 delle *"Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria"* (in G.U. n. 12 del 15/01/2019), l'Avvocato può fornire l'informativa sul trattamento dei dati personali e le notizie relative alle indagini difensive:

- in un unico contesto;
- mediante affissione nei locali dello studio;
- pubblicando la stessa informativa sul proprio sito Internet (se ne dispone);
- utilizzando formule sintetiche e colloquiali.

Per quanto concerne l'informativa ex art. 14 GDPR, il par. 5 lett. d) di tale norma prevede un'esenzione qualora i dati debbano rimanere riservati in ossequio all'obbligo di segreto professionale: caso che si attaglierebbe alla nostra professione.

In ogni caso, qualora si disponga di un sito web, sarebbe opportuno pubblicare sul sito l'informativa ex art. 14.

D: Come deve essere fornita l'informativa?

R: Il GDPR prevede che l'informativa possa essere fornita per iscritto o con altri mezzi anche elettronici (inviata via mail ad esempio) e che, su richiesta dell'interessato, possa essere fornita anche oralmente.

In ogni caso il Garante(Provvedimento 7 marzo 2019 [docweb n. 9091942] ha indicato che *Riguardo alle modalità con cui fornire l'informativa, alla luce del principio di responsabilizzazione di cui all'art. 5 del Regolamento, spetta al titolare scegliere le modalità più appropriate al caso di specie, tenendo conto di tutte le circostanze del trattamento e del contesto in cui viene effettuato (ad esempio, il dispositivo utilizzato, la natura dell'interazione con il titolare e le eventuali limitazioni che implicano tali fattori; cfr. considerando nn. 58 e 60).*

D: Quali sono le condizioni di liceità del trattamento?

R: Ai sensi dell'art. 6 del GDPR le condizioni di liceità del trattamento possono essere suddivise in due macrocategorie, una che richiede il consenso dell'interessato e una che prescinde dal consenso dell'interessato. Questa seconda macrocategoria comprende i casi in

cui il trattamento abbia come base giuridica, tra le altre, l'esecuzione di un contratto, di misure precontrattuali o un obbligo di legge.

Per quanto riguarda in generale i trattamenti svolti dagli Avvocati la condizione di liceità potrà essere rinvenuta in questa seconda macrocategoria e è corretto ritenere che sia sufficiente il generico riferimento ai *"rapporti contrattuali"* (nel caso dell'Avvocato, al mandato) ovvero alla normativa in essere (senza puntuale indicazione dei relativi riferimenti).

Ad esempio, i dati trattati per lo svolgimento dell'incarico saranno trattati per l'esecuzione del contratto, mentre la conservazione dei dati dei clienti potrà avvenire per rispettare obblighi normativi di natura fiscale.

A tal proposito il Gruppo di Lavoro sull'art. 29 in materia di consenso [7] ha ritenuto che, in genere, nell'informativa non è necessario specificare gli estremi delle norme di riferimento, ma è sufficiente l'indicazione che il trattamento è effettuato sulla base del contratto in essere con l'interessato e dei correlati obblighi normativi, anche di natura amministrativa e contabile.

In conclusione, nel caso degli Avvocati, come condizione di liceità del trattamento, nell'informativa, si potrà fare riferimento al mandato/procura in essere tra le parti ed al raggiungimento dello scopo per cui esso è conferito, nonché agli obblighi normativi cui l'avvocato è tenuto.

D: Cosa è il consenso?

R: Il *"consenso"* è la libera espressione della volontà del soggetto interessato di accettare esplicitamente il trattamento dei propri dati personali da parte del Titolare del trattamento.

Esso può essere ottenuto sia in forma scritta, che orale.

Tuttavia, onere della prova della sussistenza del consenso al trattamento prestato dall'interessato è in capo al titolare.

Dunque, è preferibile ottenere il consenso per iscritto.

In qualsiasi momento, l'interessato può revocare il proprio consenso, senza che questo pregiudichi la liceità del trattamento già effettuato precedentemente.

D: Come deve essere acquisito il consenso?

(7) *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051*

R: I requisiti dell'informativa e del consenso rimangono sostanzialmente identici a quelli previsti dalla normativa previgente in Italia (d.lgs. n. 196/2003) e dai provvedimenti del Garante in materia.

Il consenso presuppone una informativa chiara e comprensibile.

Esso può essere integrato nel modulo dell'informativa o essere inserito in un elemento esterno alla stessa, che rinvii all'informativa. Nel caso in cui l'Avvocato debba acquisire il consenso per il trattamento di alcune categorie particolari di dati per cui non vi siano altre basi giuridiche del trattamento, il consenso potrebbe, ad es., essere inserito, per comodità, nel mandato/procura.

* * * *

4. — IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO (8)

(a cura degli Avv.ti Gennaro Maria AMORUSO, Leila TESSAROLO e Caterina TOSATTI)

D: Che cos'è il registro delle attività di trattamento?

R: Il Registro delle attività di trattamento è un documento, cartaceo o elettronico, che il Titolare del trattamento utilizza per dimostrare di aver adottato una modalità di trattamento rispettosa di quanto previsto dal GDPR; costituisce, infatti, uno degli elementi della c.d. *"accountability"* (*"affidabilità"* o *"responsabilizzazione"*) del Titolare.

Si tratta di un elenco delle attività che il Titolare svolge e che hanno per oggetto il trattamento di dati personali; lo stesso viene creato *una tantum*, fotografando l'attività del Titolare e va aggiornato ogni qualvolta, a seguito di modifiche normative o organizzative, il Titolare debba eliminare un certo trattamento, ovvero eseguirne uno ulteriore o modificare le modalità di svolgimento.

D: A cosa serve il registro delle attività di trattamento?

R: Il Registro delle attività di trattamento permette, in primo luogo, di avere contezza di quali siano i trattamenti di dati personali eseguiti nel corso della propria attività, di come vengano gestiti e delle azioni da intraprendere. Esso, infatti, è una rappresentazione dei diversi tipi di trattamento che il titolare compie e permette di verificare la loro liceità, nonché la sussistenza del rischio che deve essere affrontato.

---

(8) Cfr. artt. 30 e Considerando 82 GDPR; *https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento; https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili#registro; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045*

Il Registro ha, inoltre, una funzione probatoria, essendo la misura che testimonia un trattamento lecito e trasparente ed è strumento di *'collaborazione'* con l'Autorità di controllo, ossia il Garante per la Protezione dei Dati Personali.

D: Quando è obbligatorio il registro delle attività di trattamento?

R: Il Registro risulta obbligatorio solo in determinate circostanze, anche se è certamente raccomandato per ogni trattamento (cfr. Guida all'Applicazione del Regolamento UE 2016/679 in materia di protezione dei dati personali, pubblicata sul sito del Garante Privacy) ([9]).

Secondo le indicazioni fornite sia dal GDPR, sia dal Garante, tutti i Titolari di trattamento devono adottare e tenere il Registro dei Trattamenti, qualora eseguano trattamenti non occasionali di dati personali, oppure qualora trattino dati *'particolari'* e dati relativi a condanne penali.

Vi è anche obbligo del Registro per chi abbia più di 250 dipendenti.

In particolare, il Garante, nelle proprie *"FAQs sul Registro delle attività di Trattamento"*([10]) ha ritenuto che siano obbligati ad istituirlo i *"liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati"*; tuttavia, lo stesso Garante ha, altresì, raccomandato l'adozione del Registro da parte di qualsiasi Titolare, a prescindere dai requisiti previsti per l'obbligatorietà.

D: Chi deve redigere il registro delle attività di trattamento?

R: Il Registro deve essere redatto dal Titolare del trattamento.

Nel caso in cui sia designato un DPO, tale incombenza può essere svolta dal DPO medesimo, ma sempre e comunque sotto la responsabilità del Titolare o del Responsabile (cfr. par. 4.5. delle Linee guida WP243) ([11]).

D: Cosa deve contenere il registro delle attività di trattamento?

R: In primo luogo, nel registro occorre individuare le varie attività svolte dal Titolare che comportano il trattamento di dati personali (a titolo meramente esemplificativo, si considerino, in uno studio legale: l'attività giudiziale; l'attività stragiudiziale; le agende e calendari analogici e digitali; la contabilità e la fatturazione; le comunicazioni; l'archiviazione

---

([9]) *https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali*

([10]) *https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento*

([11]) *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048*

delle pratiche; la gestione del personale dipendente e dei collaboratori; i rapporti con i fornitori; il trattamento dei dati raccolti attraverso il sito web; l'attività di marketing, nella misura in cui è consentita dal Codice Deontologico).

Nel Registro devono essere inseriti il nominativo e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati.

Inoltre, per ogni attività di trattamento, devono essere inserite delle specifiche informazioni, ossia:

- le finalità del trattamento, ossia lo scopo per cui un determinato trattamento viene effettuato. Il Garante, nelle FAQs ([12]), ha specificato che devono essere indicate anche le basi giuridiche del trattamento *ex* art. 6 GDPR o, nel caso di trattamenti di *"categorie particolari di dati"*, *ex* art. 9 GDPR, o ancora, nel caso di trattamenti di dati relativi a condanne penali e reati, la normativa che ne autorizza il trattamento, *ex* art. 10 GDPR;
- una descrizione delle categorie di interessati (es. clienti, dipendenti, fornitori) e delle categorie di dati personali trattati (ad es., dati anagrafici, dati di contatto, dati sanitari, dati giudiziari, ecc.);
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali. Tra i destinatari risulta opportuno indicare non solo i titolari cui i dati devono essere comunicati (es. enti previdenziali, autorità giudiziarie), ma, altresì, i responsabili (o sub responsabili) del trattamento;
- l'indicazione dell'eventuale trasferimento di dati verso un Paese terzo o un'organizzazione internazionale e l'indicazione del Paese terzo o dell'organizzazione internazionale in cui vengono trasferiti e le garanzie adottate ai sensi del capo V del GDPR;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati o, comunque, se non è possibile stabilire un termine massimo, i criteri in base ai quali determinare i tempi di conservazione (ad es., normativa che prevede un determinato termine);
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, par. 1, GDPR. Le misure di sicurezza dovranno essere indicate in maniera generica e approssimativa, eventualmente facendo riferimento ad altri documenti più completi e analitici.

([12]) *https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento*

Oltre alle informazioni obbligatorie, il titolare può aggiungere tutte le informazioni che ritiene pertinenti o utili. Ad es., potrebbe essere utile inserire una sintetica valutazione dei rischi, l'eventuale svolgimento di una valutazione d'impatto, le modalità di raccolta del consenso, le modalità con cui si svolge il trattamento, le modalità di rilascio delle informazioni *ex* artt. 13 e 14 del GDPR.

D: In che formato deve essere redatto il registro delle attività di trattamento e come va conservato?

R: Il Registro deve essere redatto in forma scritta, anche in formato elettronico.

Il formato elettronico, peraltro, risulta più facilmente modificabile ed è, dunque, preferibile soprattutto in strutture che hanno una molteplicità di trattamenti.

Nessuna indicazione è fornita dal regolamento in merito alla modalità di conservazione dello stesso.

Risulta, in ogni caso, necessario che il titolare sia in grado di mostrarlo senza ritardo, in caso di richiesta del Garante.

D: Il registro delle attività di trattamento deve avere *"data certa"*?

R: Il GDPR non richiede che il registro abbia data certa.

Il Garante, però, nelle proprie*"FAQs sul Registro del Trattamento"* ([13]) ha ritenuto che il Registro deve recare, in maniera *"verificabile"*, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) e la data dell'ultimo aggiornamento.

Tenendo conto degli strumenti comunemente a disposizione da parte degli Avvocati, si ritiene che si possa senz'altro adempiere a tale incombenza, con riferimento ai documenti elettronici, attraverso l'apposizione di una marca temporale, o più semplicemente attraverso un auto-invio del documento via PEC.

D: Quando deve essere aggiornato il registro delle attività di trattamento?

R: Il Registro è considerato come uno strumento dinamico che deve essere aggiornato ogni qualvolta vi sia una modifica significativa nei trattamenti (ad es., nuovi trattamenti da inserire o trattamenti non più eseguiti) o nelle modalità di svolgimento delle attività.

In tali casi, va aggiornato senza ritardo.

([13]) *https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento*

D: Anche il Responsabile del trattamento deve redigere un registro dei trattamenti?

R: Sì. Il GDPR prevede che il Responsabile del trattamento debba tenere un Registro di tutte le attività relative al trattamento svolte per conto di un titolare.

La tenuta del registro è obbligatoria alla ricorrenza dei medesimi presupposti previsti per il registro del titolare del trattamento.

In tale caso, il Registro deve contenere:

- il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il Responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento, facendo, eventualmente, riferimento a quanto contenuto nel contratto stipulato ai sensi dell'art. 28 del GDPR;
- l'indicazione dell'eventuale trasferimento di dati verso un Paese terzo o un'organizzazione internazionale e l'indicazione del Paese terzo o dell'organizzazione internazionale in cui vengono trasferiti e le garanzie adottate ai sensi del capo V del GDPR;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1, GDPR.

Nel caso in cui uno stesso soggetto agisca in qualità di Responsabile del trattamento per conto di più soggetti quali autonomi e distinti titolari, nel Registro dovranno essere riportate le informazioni richieste con riferimento a ciascuno dei titolari.

Il Registro dovrà essere, dunque, suddiviso in tante sezioni quanti sono i titolari per conto dei quali il responsabile agisce.

D: Dove è possibile trovare un modello di registro?

R: Sul sito del Garante Privacy sono presenti dei modelli di registri del titolare e del responsabile *"semplificati"* per PMI ([14]).

* * * *

5. – SICUREZZA, DATA BREACH E VALUTAZIONE DI IMPATTO PRIVACY

(a cura degli Avv.ti William DI CICCO, Alessandro MARIANI, Sarah MASATO,

([14]) *https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento*

Massimiliano PARLA, Mario VALENTINI e Domenico VOZZA)

5.1 – VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

D. Quale è la definizione di violazione dei dati personali?

R. L'art. 4, n. 12) del Regolamento UE 2016/679 (GDPR) definisce la **violazione dei dati personali (in inglese** *"data breach")* *come "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".*

Un Data Breach impatta fortemente sul trattamento dei dati personali andando a minare i tre aspetti fondamentali su cui si fonda la sicurezza dei dati ossia:

- la **riservatezza** o confidenzialità: ai dati devono accedere sole le persone autorizzate;
- l'**integrità**: i dati non devono subire modifiche o cancellazioni non autorizzate;
- la **disponibilità**: ai dati si deve poter accedere tutte le volte in cui se ne ha bisogno.

D. Quali possono essere gli indizi e le cause di un data breach?

R. Un data breach è sia un evento **doloso** come un attacco informatico, sia un evento **accidentale** come un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente).

Nell'ambito dell'attività dell'avvocato possono presentarsi diversi eventi potenzialmente idonei a determinare una violazione dei dati (data breach).

A titolo di esempio si possono riportare gli eventi che incidono:

- sulla **riservatezza** dei dati come l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati a seguito dell'accesso non autorizzato o del furto, anche via web (hackeraggio)dei dispositivi informatici (computer fisso o portatile, tablet, smartphone, pennetta usb, CD, ecc.), delle credenziali di accesso (nome utente, password, pin), delle chiavi dell'archivio fisico, dell'agenda di studio, dei fascicoli o della documentazione contenente dati personali; la riservatezza può essere compromessa anche per eventi non dolosi come l'invio di una e-mail o di un documento a un soggetto diverso dal destinatario legittimo;
- sull'**integrità** dei dati come l'alterazione deliberata da parte di terzi estranei (sabotaggio, hackeraggio, sostituzione o alterazione di documenti informatici o cartacei), o

accidentale per disattenzione, imperizia o errore umano dei componenti dello studio, o per eventi estranei all'azione dell'uomo (p.es. un incendio, una calamità naturale o anche il semplice danneggiamento di un documento originale cartaceo durante il passaggio nella fotocopiatrice o nello scanner);

- sulla **disponibilità** dei dati come l'impossibilità temporanea o permanente di accedere ad una pratica o ad un documento per cause dolose (p.es. attacchi esterni, virus, malware, ecc.) o per cause accidentali come il malfunzionamento dei dispositivi informatici o di un gestionale, la perdita delle chiavi per accedere a un archivio cartaceo o informatico (nome utente, password, pin) oppure per eventi naturali o estranei all'azione dell'uomo come l'interruzione della linea internet, telefonica o elettrica.

D. Quali strumenti organizzati e procedurali possono aiutare a gestire un data breach?

R. L'avvocato, per il principio di accountability, nonché per responsabilità professionale, non può esimersi dall'approntare misure di sicurezza adeguate sia in ottica di prevenzione del rischio, ma soprattutto adeguate a porre rimedio ad un eventuale sinistro privacy.

Per tali ragioni, è consigliabile che l'avvocato si doti di una Procedura di Risposta al Data Breach che indichi una serie di condotte "diligenti" da attuare prontamente in risposta alla violazione subita, da parte dei dipendenti, collaboratori, praticanti e amministrativi dello studio.

Tale procedura potrà consentire all'avvocato titolare dei dati di decidere e valutare la necessità e/o l'opportunità di procedere alla notificazione all'Autorità di controllo, ovvero alla comunicazione all'interessato ai sensi degli artt. 33 e 34 GDPR.

D. Quale è la procedura di notifica della violazione dei dati personali? Quale è il contenuto della notifica?

R. L'art. 33 del GDPR, prevede che, in caso di violazione dei dati, il responsabile del trattamento, se designato, deve avvertire il titolare dell'avvenuta violazione dei dati. Quest'ultimo dovrà notificare l'evento all'autorità di controllo tranne che nel caso in cui "*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*" (es. perdita di una chiavetta usb con dati cifrati). La notifica deve avvenire "***senza ingiustificato ritardo** e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza*" il titolare. Qualora la notifica non avvenga nelle 72 ore, il titolare dovrà specificare i motivi del ritardo.

La norma prevede anche la possibilità di allegare ulteriori informazioni in un momento successivo, per cui si preferisce effettuare la notifica nelle 72 ore, anche se è incompleta.
La notifica deve avere il **contenuto** previsto dall'art. 33 del GDPR e quindi descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni 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 presso cui ottenere più informazioni; descrivere le probabili conseguenze della violazione dei dati personali; descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
La notifica deve contenere, in ogni caso, le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679 e indicate nell'allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951). È auspicabile in tal caso utilizzare per la notifica il modello allegato al provvedimento stesso. Tale modello è disponibile sul sito del Garante ed in tal caso sarà necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione.

D. Quando è prevista la comunicazione della violazione dei dati personali agli interessati?
R. La comunicazione della violazione dei dati agli interessati è prevista solo se è suscettibile di presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**. Il titolare del trattamento deve **comunicare la violazione** dei dati all'interessato **senza ingiustificato ritardo come indicato all'**art. 34 del GDPR.
L'art. 34 prevede espressamente i casi nei quali non è richiesta tale comunicazione:
a) il titolare del trattamento ha messo in atto le misure tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la **cifratura o la crittografia**;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) la **comunicazione richiederebbe sforzi sproporzionati e quindi** si procede a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione agli interessati non deve essere generica, ma deve contenere tutte le informazioni per consentire alle persone di comprendere il rischio e proteggere i loro dati e quindi dovrà contenere una descrizione della natura della violazione delle sue possibili conseguenze, e dovrà fornire precise indicazioni sugli accorgimenti da adottare per proteggersi da usi illeciti dei propri dati e per evitare ulteriori rischi.

D. Quali elementi deve contenere la comunicazione della violazione dei dati personali agli interessati?

R. Tale comunicazione deve contenere almeno:

- le informazioni del nome e dei dati di contatto del DPO (ove applicabile) o di altro punto di contatto presso cui ottenere maggiori informazioni;
- la descrizione della natura della violazione dei dati personali e delle probabili conseguenze, le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi, utilizzando un linguaggio semplice e chiaro.

5.2 — VALUTAZIONE DEL RISCHIO E DPIA

D. Data Protection Impact Assessment (DPIA): Avvocati, quando farla e perché?

R. La Valutazione d'Impatto sul trattamento dei dati personali, comunemente abbreviata nell'acronimo inglese DPIA, rappresenta uno dei principali adempimenti del Titolare del trattamento in virtù del principio di *accountability*.

Ciò in ragione del fatto che il GDPR impone un cambio di mentalità, rispetto la vecchia Direttiva Madre (Dir. 95/46/CE), in ottica preventiva - precauzionale per cui il trattamento dei dati personali va progettato e inserito in uno schema di *privacy by design* fin dall'inizio, prima cioè che questo venga effettivamente posto in essere.

Alla luce di quanto stabilito dall'art. 35 GDPR il Titolare, prima di procedere al trattamento, effettua una valutazione d'impatto sulla protezione dei dati personali, qualora un tipo di trattamento preveda l'utilizzo di nuove tecnologie, dovendo, inoltre, prendere in considerazione la natura, l'oggetto, il contesto e le finalità.

Generalmente, tale valutazione ricade su di uno specifico trattamento di dati personali sebbene, alla fine del primo paragrafo, il Legislatore europeo apra alla possibilità di far

ricadere sotto una medesima valutazione anche un insieme di trattamenti simili che presentano rischi analoghi per i diritti e le libertà delle persone fisiche.

Ebbene, la norma individua i casi di obbligatorietà della DPIA in relazione a quei trattamenti che in base alle loro caratteristiche possono risultare più pericolosi tra i quali rientrano:

a) la 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 su dette 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;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Tuttavia, il Considerando 91 del GDPR esclude per alcune figure professionali, tra le quali rientra anche quella dell'avvocato, un vero e proprio obbligo di procedere ad una DPIA, in ragione del fatto che il trattamento posto in essere da tali soggetti non è da considerarsi effettuato su larga scala.

Invero, è buona prassi anche per l'avvocato, nell'ottica di una buona *privacy diligence*, di predisporre un piano di valutazione del trattamento soprattutto in relazione ai profili di aggiornamento, manutenzione e inserimento di nuovi dispositivi e tecnologie a supporto dell'attività lavorativa di tutti i giorni.

Più precisamente, il GDPR in tema di misure di sicurezza, ci porta necessariamente all'utilizzo di dispositivi digitali in sostituzione di quelli tradizionali cartacei, data la loro maggiore sicurezza, versatilità e tracciabilità.

Pertanto, è consigliabile che in sede di aggiornamento delle infrastrutture informatiche l'avvocato si confronti con i relativi fornitori al fine di valutare la loro DPIA e di conseguenza valutare *de relato* l'impatto sulla propria attività. Tutto ciò, in quanto l'avvocato, nonostante il trattamento non possa configurarsi su "larga scala", tratta dati estremamente sensibili quali quelli giudiziari (e non solo, come nei casi di procedimenti per responsabilità medica) che necessitano, dunque, di una maggiore protezione.

D. Come condurre la Valutazione del Rischio Privacy nello studio legale?

R. Premesso che la DPIA non costituisce un obbligo dell'avvocato come Titolare del trattamento, in forza del Considerando 91 GDPR, lo studio legale, data l'estrema sensibilità dei dati a disposizione (giudiziari, ma non solo...), non può prescindere da una

pianificazione delle attività di trattamento e da una considerazione circa l'opportunità di efficientare le misure di sicurezza a disposizione.

Uno dei principali step da compiere risulta essere la valutazione del rischio, che consiste nella valutazione soggettiva ed individuale dei rischi parametrata su criteri quali la tipologia e natura dei dati trattati, il contesto, le finalità di trattamento, lo stato dell'arte e i costi di attuazione inevitabilmente diversi per ogni titolare.

Per quanto concerne la valutazione dei rischi, in termini di pericolo per i diritti e le libertà delle persone fisiche, stando al considerando 75 GDPR, vengono in rilievo tutte quelle attività di trattamento di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale significativo, privazione dei diritti e delle libertà, impedimento dell'esercizio del controllo sui dati personali; ma anche trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, relativi alla salute, vita sessuale, condanne penale e a reati o alle relative misure di sicurezza.

In merito, risulta fondamentale lo studio e l'applicazione della norma internazionale ISO/IEC 29134:2017 dal titolo "Privacy Impact Assessment - Methodology" che individua le linee guida e definisce i requisiti per una valutazione del rischio e d'impatto connessi alla protezione delle informazioni personali (prendendo, inoltre, in considerazione gli standard individuati ISO/ IEC 27001, 27002).

In tema di valutazione e gestione del rischio, rileva inoltre la norma internazionale UNI ISO 31000:2018 "Risk Management" che elabora un modello di gestione e controllo basato sullo schema PDCA (Plan - Do - Check - Act) che aiuta l'organizzazione dello studio legale a sviluppare un approccio proattivo alla gestione del rischio.

Nella valutazione dei rischi dovranno essere, poi, attenzionati i profili riguardanti la sicurezza del trattamento, e quindi distruzione, indisponibilità, perdita, integrità in termini di alterazione, riservatezza, divulgazione, accesso non autorizzato ai dati.

Una volta individuate le categorie di dati trattati, le attività di trattamento e le categorie degli interessati, si procede alla definizione del rischio legato alla gestione e al trattamento:

- i dati sensibili dei clienti e/o di terzi riguardanti lo stato di salute, o idonei a rivelare la vita sessuale, per le pratiche riguardanti la sfera personale e familiare (separazioni, divorzi, disconoscimenti di paternità);

- il rischio di accesso all'interno dello studio da parte di soggetti non autorizzati può essere definito basso se è previsto un accesso controllato da parte del personale dipendente o da incaricati nell'orario di apertura;
- il rischio per il trattamento dei dati cartacei: è basso quando l'archivio è dotato di chiusura a chiave, i fascicoli sono riposti in armadi chiusi, in appositi schedari e prelevati per il tempo necessario al trattamento, non lasciati incustoditi sulle scrivanie;
- i rischi relativi ai device: basso quando viene effettuata pulizia periodica dei file temporanei e del disco rigido; quando è vietata la navigazione in internet su siti poco attendibili o non ufficiali e si è data disposizione di non aprire e-mail provenienti da soggetti non conosciuti; policy per la creazione di password forti (combinazioni alfa-numeriche, minimo di otto caratteri, cambio password periodica ogni tre mesi);
- il rischio di deterioramento dei dati memorizzati su supporto digitale è basso vengono effettuati frequentemente operazioni di backup; quando vengono utilizzati sistemi di mass storage in criptazione forte; quando vi è utilizzo della tecnica di deframmentazione.

Queste valutazioni sugli *"effetti complessivi del trattamento"* aiuteranno il libero professionista ad individuare le attività di trattamento dei dati per le quali valutare, mitigare, gestire e minimizzare il rischio.

5.3 – MISURE DI SICUREZZA

D. Quali misure di sicurezza devono essere adottate (principio di accountability)?

R. Il GDPR stabilisce l'obbligo per il titolare del trattamento di adottare *"misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio"* (art. 32 GDPR). Nello specifico il GDPR orienta la scelta verso le misure che assicurino, se del caso:

"a) la pseudonimizzazione 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 o tecnico;

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

Oltre alle suddette indicazioni di massima, il GDPR non prevede un elenco prestabilito delle misure di sicurezza da adottare, in quanto rimette la scelta al titolare del trattamento sulla base di una sua valutazione.

Questo perché il GDPR si fonda sul principio di responsabilizzazione (*accountability*), che implica la libertà del titolare del trattamento di approntare, nei limiti del rispetto dei principi imposti dalla normativa, le misure che ritiene più adeguate alla protezione dei dati personali.

Il principio di responsabilizzazione comporta, però, anche la necessità di dover dare prova della valutazione svolta e delle scelte operate, rendendo di fatto non possibile basarsi solamente su modelli precompilati ovvero su documentazione standard.

Il GDPR indica fra gli elementi che l'avvocato dovrà considerare per la scelta delle misure di sicurezza da adottare lo *"stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche"* (art. 32).

D. cosa si intende per pseudonimizzazione e cifratura dei dati personali?

R. La pseudonimizzazione e la cifratura dei dati sono strumenti che perseguono il medesimo fine di oscurare il dato per renderlo incomprensibile a coloro che non hanno la "chiave" per accedervi, sebbene con alcune differenze.

La pseudonimizzazione è definita nel GDPR come la tecnica che permette il trattamento dei dati personali in modo tale che tali dati *"non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive"* (art. 4, punto 5).

Più semplicemente tale tecnica consiste nel sostituire i dati personali con dei codici o pseudonimi, così che un terzo non possa individuare la persona a cui si riferiscono i dati.

Per l'avvocato tale misura può, e deve, essere adottata per esempio nell'intestazione dei fascicoli di studio, sulla cui copertina è consigliabile non indicare i nomi delle parti, ma un codice o un numero di classificazione. In questo modo, solo chi è a conoscenza del codice di classificazione del fascicolo può risalire all'identità della persona a cui i dati si riferiscono.

La crittografia o cifratura, invece, si basa di solito su un algoritmo e su una password.

Con la crittografia un qualunque file di dati (testo, immagini, ecc.), con l'utilizzo di un algoritmo, viene trasformato in un insieme di segni e simboli assolutamente privi di significato che potranno essere decifrati e resi leggibili solo con l'utilizzo della "chiave" giusta. In questo modo, anche se un estraneo accede ai file o al dispositivo protetto da cifratura, non potrà visualizzare i dati se non in possesso della password.

D. Cosa si intende per *"capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"* di cui all'art. 32, par. 1, lettera b), GDPR?

R. L'art. 32 par. 1 lettera b) fa riferimento ai concetti di riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi informatici che trattano i dati personali.

Per riservatezza si intende la protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la lettura da parte di persone non autorizzate.

Per integrità, si intende la conferma che i dati trasmessi, ricevuti o conservati siano completi e inalterati.

La disponibilità, invece, è da intendersi come conferma che i dati siano accessibili e i servizi funzionino anche in caso di interruzioni dovute a eventi eccezionali o ad attacchi di pirateria informatica.

Con il concetto di resilienza, infine, ci si riferisce alla capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura al fine di assicurare la disponibilità dei servizi che vengono forniti e l'adeguata protezione dei dati che vengono trattati con tali sistemi.

D. Cosa si intende per *"capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico"* di cui all'art. 32, par. 1, lettera c), GDPR?

R. La norma di cui all'art. 32 par. 1 lettera c) GDPR attribuisce rilievo al concetto di *disaster recovery*, che consiste nella capacità di reagire in modo efficace e tempestivo ad eventuali criticità dovute ad incidenti fisici o tecnici, allo scopo di ripristinare la disponibilità e l'accesso dei dati personali oggetto di trattamento.

A tale riguardo, sarà quindi importante per i titolari predisporre un programma specifico attraverso cui analizzare innanzitutto i rischi che potrebbero andare a colpire il sistema informatico; prevedere poi le adeguate misure da adottare per minimizzarli; ed infine predisporre un piano di emergenza che permetta di attuare un sistema alternativo di elaborazione dei dati da utilizzare in attesa della completa riattivazione.

D. Quali sono le misure da adottare per i documenti e fascicoli gestiti digitalmente?

R. Per la gestione dei documenti e fascicoli digitali, si consiglia di:

- impostare un sistema di autenticazione: prevedere l'accesso tramite una password diversa per ogni avocato e collaboratore;
- gestire e profilare gli accessi: prevedere che le persone accedano ai soli dati di cui hanno necessità per il proprio lavoro ed evitare che tutti accedano a tutto indiscriminatamente e rimuovere le autorizzazioni obsolete;
- impostare un sistema di backup: evitare che i documenti e i fascicoli digitali siano conservati su un unico computer, ma prevedere un sistema di copia o sincronizzazione dei dati su un altro supporto custodito;
- proteggere gli strumenti informatici: dotarsi di software di protezione contro le minacce informatiche (antivirus, antimalware, firewall, ecc.);
- mantenere in efficienza gli strumenti informatici: installare e utilizzare solo software sicuri e prevedere il periodico aggiornamento e manutenzione dei dispositivi hardware e dei software utilizzati;
- gestire i dispositivi mobili: prevedere un sistema di protezione adeguato (password, crittografia, ecc.) per computer portatili, smartphone, chiavette USB, CD, DVD, tablet, hard disk portatili, ecc., ed evitare, per quanto è possibile, di memorizzare su tali dispositivi dati personali sensibili dei clienti e comunque prevedere un sistema di copia e sincronizzazione (backup) dei dati presenti anche su altri supporti custoditi a studio;
- gestire la dismissione e manutenzione degli strumenti informatici: se si dismette definitivamente un dispositivo (p.es. smartphone, tablet, pennetta usb, ecc.) si dovrà procedere alla cancellazione definitiva dei dati presenti o, se non è possibile, bisognerà rendere inutilizzabile il dispositivo. In caso di malfunzionamento dei dispositivi si consiglia di rimuovere i dati presenti prima di consegnarlo ad un tecnico per la riparazione e comunque di affidarsi all'assistenza di personale e società qualificate che assicurino non solo un intervento a regola d'arte, ma anche le dovute rassicurazioni sulla sicurezza dei dati presenti.

D. Quali password scegliere e come gestirle?

R. Per accedere agli strumenti informatici (dispositivi, e-mail, programmi, gestionali, ecc.), si dovrà adottare una password "sicura" diversa per ogni persona e per ogni tipologia di accesso. Si consiglia di utilizzare una password composta da almeno 8 caratteri alternando lettere minuscole e maiuscole, numeri e caratteri speciali che non possa essere scoperta da un

programma o da una persona in un breve lasso, ma che nello stesso tempo sia facile da ricordare.

La password non dovrà essere condivisa e non dovrà essere scritta chiaramente su un foglio e andrà cambiarla regolarmente.

Fra i metodi per creare una password sicura e facile da ricordare vi è quello di partire da una frase piuttosto che da una singola parola complessa, provvedendo a modificare alcune lettere in modo che non rimanga di senso compiuto.

Per una password sicura si consiglia di:

- non utilizzare le stesse password per più account o utilizzate negli account personali (p.es. social network, e-mail privata, sito per hobby privati, ecc.);
- non scegliere una password contenente riferimenti agevolmente riconducibili alla persona o ai suoi famigliari oppure in generale a parole a lei riconducibili (p.es. codice fiscale, nome della moglie o dei figli, luogo e data di nascita, ecc.);
- non utilizzare parole di uso comune (nomi di luoghi, personaggi, mesi, giorni della settimana, ecc.) o acronimi che si possono trovare nel dizionario, anche in lingue straniere;
- non prevedere citazioni, slogan, motti o detti conosciuti;
- non utilizzare sequenze di tasti sulla tastiera (asdf) o sequenze di numeri (1234);
- non impostare password di soli numeri, di sole lettere maiuscole o di sole lettere minuscole;
- non prevedere ripetizioni di caratteri (aa11);
- non utilizzare password adottate in precedenza;
- non adottare una password utilizzata in un esempio trovato di come si sceglie una buona password.

D. Quali misure di sicurezza adottare nell'utilizzo della posta elettronica e di Internet?

R. Nell'utilizzo delle e-mail e di internet, al fine di garantire la massima protezione dei dati trattati e degli strumenti utilizzati è consigliabile adottare le seguenti misure di sicurezza e buone prassi:

- scegliere un provider di posta elettronica che fornisca le dovute rassicurazioniin merito a sicurezza e competenza;
- utilizzare un account di mail specificatamente ed esclusivamente dedicato all'attività professionale;

- evitare di fornire la propria mail per iscriversi a portali, newsletter o servizi non attinenti all'attività di lavoro o che non assicurino un livello adeguato di sicurezza;
- evitare di aprile le e-mail non richieste, quelle provenienti da persone sconosciute, quelle con contenuto anomalo, quelle classificate come "spam" e quelle provenienti da enti, uffici o società (p.es. banche, Agenzia delle entrate, Inps, Inail) che normalmente utilizzano pec e non e-mail; nel dubbio è consigliabile accedere attraverso il portale ufficiale del mittente piuttosto che utilizzare il link indicato nella mail sospetta;
- evitare di scaricare file, link o programmi allegati alla posta elettronica di cui non è sicuro della provenienza o presenti su siti internet non attendibili o inaffidabili (spesso gratuiti) come siti freeware o shareware. Non installare automaticamente le opzioni predefinite (barre degli strumenti, componenti aggiuntivi, plugin, motori di ricerca, ecc.);
- evitare di fornire o comunicare con e-mail o su internet informazioni o dati relativi a password o credenziali di accesso ai propri dispositivi;
- se si deve inviare uno stesso allegato a più persone, è consigliabile non lasciare in chiaro gli indirizzi e-mail di tutti i destinatari, a meno che i destinatari si conoscano fra loro e si tratti di una discussione comune a tutti (si ricorda che anche gli indirizzi e-mail sono da ritenersi dati personali);
- se si devono inviare allegati diversi a più soggetti, si consiglia di inviare e-mail separate per ogni destinatario con il rispettivo allegato. Inoltre, se non espressamente previsto e autorizzato, non si dovranno inviare dati personali attinenti a soggetti terzi rispetto al destinatario della e-mail e se tali dati sono contenuti in uno stesso file (p.es. elenco di nomi, indirizzi ecc.), si dovranno mantenere separati i rispettivi dati personali o rimuovere i dati personali non attinenti al singolo destinatario;
- utilizzare sempre le connessioni sicure per inviare le mail e navigare su internet ed evitare di connettere i dispositivi a reti wi-fi pubbliche, hotspot o reti non protette.

D. Quali sono le misure di sicurezza da adottare per i documenti, archivi e fascicoli cartacei?

R. Per la gestione dei documenti, archivi e fascicoli cartacei, si consiglia di:

- evitare di indicare sulle copertine dei fascicoli i dati personali delle parti (p.es. nome, cognome, indirizzo, cod. fiscale ecc.), ma utilizzare una sigla o codice sostitutivo in base alla classificazione adottata dallo studio (c.d. pseudonimizzazione);

- evitare di lasciare incustoditi i documenti e fascicoli sulla propria scrivania o in altri luoghi dello studio, ma riporli negli appositi archivi o cassetti da mantenere chiusi, soprattutto se nello studio accedono persone estranee (p.es. addetti alle pulizie, collaboratori occasionali, fornitori di servizi, ecc.);
- evitare di lasciare incustoditi i documenti nella stampante o nello scanner quando a tali dispositivi accedono anche terze persone;
- se è necessario inviare documenti contenenti dati personali di più persone, se non espressamente necessario, è consigliabile mantenere separati i rispettivi dati personali o rimuovere i dati personali non attinenti al destinatario formando tante copie differenti (p.es. formando tanti estratti o copie del documento in modo che ogni destinatario riceva solo i dati che gli riguardano);
- è consigliabile non stampare, estrarre o fotocopiare documenti con dati personali se non strettamente necessario alla finalità dell'incarico;
- è consigliabile custodire i fascicoli e i documenti in archivi e/o armadi dotati di serrature e chiavi;
- è consigliabile portare fuori dai locali dello studio fascicoli e documenti contenenti dati personali se non strettamente necessario e comunque con la massima attenzione e custodia;
- è consigliabile non portare i fascicoli e i documenti fuori dai locali dello studio, se non necessario allo svolgimento dell'incarico e in tal caso, se non è strettamente necessario, evitare di portare fuori gli originali. In ogni caso è consigliabile custodire con attenzione i fascicoli e i documenti, evitando di lasciarli in luoghi non sicuri (p.es. in macchina, in luoghi pubblici, presso un cliente, ecc.);
- riporre in modo ordinato i documenti negli appositi fascicoli e poi negli appositi archivi o cassetti, in maniera che possano essere reperiti facilmente;
- evitare di passare i documenti originali nelle macchine fotocopiatrici, scanner, fax, fascicolatori o altri macchinari se vi è il rischio di inceppamento e danneggiamento del documento (p.es. evitare di far passare i documenti originali attraverso il vassoio automatico della fotocopiatrice, ma utilizzare l'opzione manuale a vetro fotocopiando un documento alla volta);
- formare e informare i colleghi, collaboratori e le persone che accedono allo studio su tali regole e misure.

D. Si può utilizzare un servizio cloud? E con quali accortezze?

R. Il GDPR non vieta l'utilizzo di servizi cloud, ma l'avvocato dovrà comunque tutelare e proteggere i dati personali, verificando la presenza di adeguate garanzie di sicurezza, soprattutto perché spesso l'offerta di servizi cloud si fondano su condizioni di contratto predisposte dagli stessi fornitori la cui negoziabilità è quantomeno limitata, specialmente per quanto attiene agli standard di sicurezza.

Pertanto, prima di utilizzare un servizio cloud su cui trasferire i dati personali dei propri clienti, è consigliabile analizzare alcuni aspetti relativi:

- alla gestione e *"destino"* dei dati personali alla cessazione del rapporto contrattuale;
- all'ubicazione dei server dove sono conservati i dati e ai possibili trasferimenti extra-UE (p.es. per la presenza di subappaltatori del fornitore);
- alla possibilità, da parte del fornitore dei servizi cloud di monitorare l'utilizzo dei servizi da parte dell'utente e la possibilità di un accesso e trattamento di dati personali;
- alla possibilità per l'avvocato-utente di poter effettuare audit precontrattuali, test, o verifiche sul fornitore ed eventuali subfornitori dei servizi cloud;
- alla verifica che le politiche (policy) di sicurezza applicate dal fornitore dei servizi cloud siano in linea con le prescrizioni del GDPR e con gli standard di sicurezza riconosciuti (p.es. ISO 27001) o siano avvalorati con certificazioni rilasciate da organismi tersi indipendenti;
- all'obbligo da parte del fornitore dei servizi cloud di segnalare tempestivamente e in modo circostanziato eventuali violazione dei dati (data breach);
- alla possibilità per l'avvocato-utente di richiedere la copia dei dati trasferiti in un formato facilmente fruibile (portabilità dei dati), ad esempio, per l'esigenza di poter migrare i dati in un altro servizio cloud senza rischiare di perdere i dati.

Pertanto, l'avvocato che intende utilizzare un servizio cloud è tenuto ad effettuare una verifica accurata sul fornitore (due diligence) per valutare se il fornitore è in grado di soddisfare non solo le esigenze operative, ma anche quelle di sicurezza dei dati personali trattati.

È consigliabile comunque conservare una copia dei dati anche su supporti da custodire all'interno dello studio.

Non deve, comunque, trascurarsi che il ricorso ai servizi cloud presenta diversi vantaggi, anche perché le infrastrutture e i livelli di sicurezza offerti dai fornitori di servizi cloud

spesso risultano difficilmente replicabili all'interno dello studio, se non con importanti investimenti di risorse non sempre alla portata dei piccoli e medi studi legali.

5.4 – IL SITO WEB DELLO STUDIO LEGALE

D. quali sono le attività che deve compiere l'avvocato in caso di raccolta di dati personali attraverso il sito internet?

R. Il sito web può essere utilizzato dall'avvocato per promuovere la propria attività professionale, per presentare i componenti dello studio, pubblicare articoli, ma anche consentire la raccolta di dati personali mediante un questionario online, una consultazione online, un modulo di contatto, la creazione di un account online, nonché attraverso i cookies.
Se il sito web dello studio permette l'inserimento di dati personali, ad esempio il modulo di contatto e richiesta informazioni, è opportuno che sia utilizzata la connessione con protocollo sicuro HTTPS (tecnologia "SSL") per garantire il rispetto delle misure di sicurezza in funzione della confidenzialità delle informazioni scambiate con il professionista.
L'avvocato dovrà inserire, all'interno del registro delle attività di trattamento, un apposito modulo dedicato al trattamento dei dati personali sul sito web.
Siffatto modulo dovrà contenere l'indicazione di:

- identità e dettagli di contatto del titolare;
- scopi;
- categorie di persone;
- categorie di dati personali;
- categorie di destinatari;
- trasferimenti verso un paese terzo o un'organizzazione internazionale;
- scadenze per la cancellazione;
- descrizione generale delle misure di sicurezza tecniche e organizzative.

Ai sensi dell'art. 23 del Codice Deontologico, inoltre, nel caso in cui l'avvocato riceva una proposta di incarico tramite il sito web ha l'obbligo di formalizzare il mandato accertando l'identità del cliente.

D. Quali sono i dati obbligatori che l'avvocato deve necessariamente includere nel sito web?

R. Il sito web del professionista deve contenere alcuni dati obbligatori.

Tali elementi obbligatori sono previsti:

- dal Codice deontologico, quali l'indicazione del titolo professionale, la denominazione dello studio e l'ordine di appartenenza ex art. 35, comma 3 del Codice Deontologico.
  Ai sensi dell'art. 35, comma 5 del Codice Deontologico il praticante può utilizzare soltanto il titolo per esteso "praticante avvocato" con l'eventuale indicazione di "abilitato al patrocinio" qualora abbia conseguito l'abilitazione;
- dall'art. 7 del D. Lgs. n. 70/2003 sul commercio elettronico (che prevede l'irrogazione di una sanzione amministrativa da Euro 103 ad Euro 10.000), quali il riferimento alle norme professionali e al codice deontologico e le modalità di consultazione dei medesimi, nonché il numero della partita IVA. In base a quanto disposto dalla Legge n. 247/2012 il compenso non è tra le informazioni che possono essere diffuse;
- dal GDPR, quali l'obbligo incombente per i titolari di siti web di informare gli utenti che visitano il sito sulle modalità di utilizzo dei cookie, l'Informativa sul trattamento dei dati e le informazioni di cui agli artt.13 e 14 GDPR.

D. In caso di utilizzazione dei cookies l'avvocato come deve rendere la relativa informativa?

R. In primis, l'avvocato dovrà verificare l'effettiva presenza di cookie sul sito web attraverso il dipartimento IT del provider, attraverso i fornitori di servizi o controllando gli strumenti utilizzati per la messa a disposizione del sito web.

Successivamente, è necessario determinare i tipi di cookie utilizzati sul sito web dell'avvocato.

Alcuni cookie richiedono il consenso dell'utente, come i cookie pubblicitari, i cookie *"social network"* generati dai pulsanti di condivisione, quando raccolgono dati personali senza il consenso delle persone interessate, ed alcuni cookie di misurazione degli accessi.

In questo caso, il consenso deve essere precedente all'inserimento o alla lettura del contenuto del sito. Finché il cliente non ha dato il suo consenso, questi cookie non possono essere depositati o letti dal sito stesso.

* * * *

6. – MEZZI DI RICORSO E SANZIONI

(a cura degli Avv.ti Daniela BIANCHINI, Elena IEMBO e Loredana QUASSINTI)

D: L'avvocato titolare del trattamento dei dati personali di un cliente (o anche di un dipendente dello studio) è tenuto a dare ulteriori informazioni in merito alle modalità di trattamento dei dati dopo l'acquisizione del consenso da parte dell'interessato?

R: Sì. Ogni persona può infatti tutelare i propri dati personali esercitando i diritti previsti dal Regolamento, fra cui anche quello relativo alla richiesta di informazioni in ordine al trattamento (cfr. artt. 15-22: diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione del trattamento...).

L'interessato quindi, anche dopo aver prestato il consenso al trattamento dei propri dati ed avendo acquisito in quella sede le informazioni circa le modalità con cui vengono trattati i suoi dati, può comunque rivolgere successivamente un'istanza all'avvocato titolare del trattamento per chiedere ulteriori informazioni, più o meno dettagliate a seconda delle esigenze, sulle concrete ed attuali modalità di trattamento.

L'art. 2 *terdecies* del D.Lgs 101/2018 prevede, inoltre, che i diritti di cui agli articoli da 15 a 22 del Regolamento UE 2016/679 (concernenti il diritto di accesso, rettifica, integrazione, oblio, portabilità) riferiti ai dati personali concernenti persone decedute possano essere esercitati «*da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione*».

Il secondo comma dell'art. 2 *terdecies*, tuttavia, esclude l'esercizio dei diritti di cui sopra nei casi previsti dalla legge (si pensi ad informazioni soggette ad un particolare regime di segretezza per esigenze di ordine pubblico) e qualora, limitatamente all'offerta diretta di servizi della società dell'informazione, sia stato l'interessato, ossia il defunto, a precluderne l'esercizio.

L'istanza non richiede particolari formalità e può essere trasmessa mediante lettera raccomandata o anche semplicemente a mezzo fax o posta elettronica.

D: L'avvocato titolare del trattamento, in caso di modifiche nel trattamento dei dati successive all'acquisizione del consenso, ha l'obbligo di effettuare le relative comunicazioni ai diversi interessati, a prescindere da eventuali richieste da parte di questi ultimi?

R: Sì. Nel rispetto dei principi di correttezza e trasparenza e ai sensi degli artt. 13 e 14 del GDPR, si ritiene corretto che il titolare del trattamento comunichi tempestivamente ai diversi interessati eventuali modifiche, successive all'acquisizione del consenso, concernenti il trattamento dei dati. Ad esempio, qualora nell'informativa sia stato fornito il nominativo del

Responsabile del trattamento, laddove venga nominata in seguito una persona diversa, è opportuno che il Titolare provveda a darne informazione agli interessati.

D: Cosa deve fare l'avvocato in seguito alla ricezione di una richiesta di informazioni circa il trattamento dei dati?

R: L'avvocato titolare del trattamento deve fornire un riscontro adeguato, rispondendo in maniera puntuale alle domande contenute nell'istanza.

Ai sensi dell'art. 12.3 del Regolamento, se è stata presentata un'istanza mediante mezzi elettronici, le informazioni possono essere fornite con i medesimi mezzi, qualora sia possibile, salvo diversa indicazione dell'interessato.

D: È previsto un termine entro cui il titolare del trattamento è tenuto a dare una risposta?

R: Sì. L'art. 12.3 del Regolamento prevede che il titolare del trattamento fornisca all'interessato le informazioni relative all'azione intrapresa «*senza giustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa*». Qualora il termine di un mese non fosse sufficiente, in considerazione della complessità e del numero di richieste, il titolare del trattamento dovrà comunque rispondere entro un mese dal ricevimento della richiesta, informando l'interessato della necessità di un tempo maggiore per la risposta, spiegandone altresì i motivi. La proroga non potrà comunque essere superiore a due mesi.

D: Il titolare del trattamento può esimersi dal rispondere?

R: No. Qualora il titolare del trattamento non ritenesse di dover ottemperare alla richiesta dell'interessato, ai sensi dell'art. 12.4 dovrà comunque informarlo senza ritardo (al più tardi entro un mese dal ricevimento della richiesta) della decisione, spiegando i motivi dell'inottemperanza e informando l'interessato della possibilità di proporre reclamo al Garante per la protezione dei dati personali (o ad altra Autorità di controllo competente) o di proporre ricorso giurisdizionale.

D: I costi relativi alle informazioni richieste al titolare del trattamento da chi sono sostenuti?

R: Ai sensi dell'art. 12.5 del Regolamento, le informazioni e le eventuali comunicazioni sono gratuite per gli interessati. Tuttavia, nel caso di richieste manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può

addebitare un contributo spese in base ai costi amministrativi sostenuti oppure rifiutare di soddisfare la richiesta, dandone relativa comunicazione nei termini di cui all'art. 12.3 del Regolamento.
In ogni caso, il titolare del trattamento ha l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

D: Qualora l'interessato non fosse soddisfatto della risposta fornita dal titolare del trattamento o in caso di mancato riscontro entro i termini stabiliti, quali strumenti sono previsti a tutela dell'interessato?
R: L'interessato, ai sensi dell'art. 140 bis del Codice privacy, può scegliere alternativamente se rivolgersi all'Autorità giudiziaria mediante ricorso o al Garante per la protezione dei dati personali mediante reclamo. Non può essere proposto reclamo al Garante qualora per il medesimo oggetto e fra le medesime parti sia stata già adita l'autorità giudiziaria.

D: In seguito alla presentazione del reclamo, come procede il Garante?
R: In seguito alla presentazione del reclamo al Garante vi sarà un'istruttoria e un eventuale successivo procedimento amministrativo, all'esito del quale il Garante, ritenute fondate le doglienze dell'interessato, potrà adottare nei confronti del titolare i provvedimenti di cui all'art. 58 del Regolamento. Avverso la decisione del Garante è ammesso il ricorso giurisdizionale ai sensi degli articoli 143 e 152 del Codice privacy e dell'art. 78 del Regolamento.

D: Qualora l'interessato, all'esito della risposta fornita dal titolare, ritenesse non corretto il trattamento dei propri dati personali, quali strumenti potrebbe esercitare a sua tutela?
R: L'interessato può scegliere alternativamente se agire mediante ricorso innanzi all'Autorità giudiziaria o presentare reclamo al Garante per la protezione dei dati personali.

D: Qualora l'interessato intendesse agire innanzi all'Autorità giudiziaria per il risarcimento del danno, o presentare reclamo al Garante, quali potrebbero essere i soggetti chiamati a rispondere?
R: Ai sensi dell'art. 82 del Regolamento, «*chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento, ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*». Va però considerato che, ai sensi dell'art. 82.2, il titolare del trattamento risponde per il danno cagionato dal suo trattamento

che sia stato effettuato in violazione della normativa sulla privacy, mentre il responsabile del trattamento risponde per il danno causato dal trattamento solo in caso di mancato adempimento degli obblighi previsti specificamente per i responsabili del trattamento oppure se ha agito in maniera difforme o contraria rispetto alle legittime istruzioni fornitegli dal titolare del trattamento.

Pertanto, laddove l'avvocato titolare del trattamento abbia conferito formale incarico ad un soggetto terzo rispetto allo studio (es: consulente del lavoro, commercialista, consulente di parte, interprete, amministratore del sistema ecc.) di trattare per suo conto dati personali, anche questi in qualità di responsabile del trattamento potrà essere chiamato a rispondere del danno, limitatamente a quanto sopra indicato.

È inoltre previsto dal Regolamento che i soggetti tenuti al risarcimento del danno sono responsabili in solido per l'intero ammontare. Il GDPR, all'art. 82 e al considerando 146, stabilisce che l'interessato, qualora si ritenga leso nei propri diritti da un trattamento illecito, possa rivolgersi indifferentemente tanto al titolare quanto al responsabile coinvolti nel trattamento. Tale previsione è finalizzata a garantire all'interessato il *"pieno ed effettivo"* indennizzo del danno subito, per l'intero ammontare. Nei rapporti interni, la regola è invece quella della responsabilità pro quota, per cui l'avvocato titolare o il responsabile (come sopra delineato) che abbia risarcito integralmente l'interessato potrà agire in regresso nei confronti dell'altro, o degli altri obbligati solidali, qualora ritenga che vi sia stata una responsabilità concorrente o esclusiva di questi nella produzione del danno. È evidente l'importanza che riveste per ogni obbligato coinvolto nel trattamento la circostanza di poter dimostrare l'adozione di misure adeguate rispetto al rischio insito nello specifico trattamento e volte a prevenire il danno cagionato. È ancora l'articolo 82, al paragrafo terzo, a sancire, infatti, che il titolare o il responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è a loro imputabile.

È bene anche ricordare che, pur in presenza di una violazione della normativa a tutela dei dati personali, l'interessato che voglia richiedere il risarcimento di un pregiudizio subito dovrà provare, oltre alla violazione, l'esistenza stessa del danno e il nesso causale tra questi elementi. In presenza di un trattamento illecito l'unica conseguenza davvero ineliminabile è la inutilizzabilità dei dati trattati, con l'unica riserva (ex art. 160-bis Codice Privacy) relativa alla validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme che restano disciplinate dalle pertinenti disposizioni processuali.

Per quanto riguarda il reclamo al Garante, questo potrà coinvolgere sia l'avvocato titolare del trattamento, sia il soggetto terzo allo studio al quale l'avvocato titolare del trattamento abbia conferito formale incarico di trattare i dati personali del cliente, in qualità di responsabile del trattamento.

D: In presenza di una violazione della normativa a tutela dei dati personali chi può azionare i mezzi di tutela previsti?

R: Il D.lgs. 101/2018 è intervenuto anche su questa parte del "Codice Privacy" modificando in toto l'art. 142,Titolo I, Capo I, relativo alla tutela davanti al Garante, prevedendo espressamente nel nuovo testo che *«il reclamo è sottoscritto dall'interessato o, su mandato di questo, da un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117,che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati, con riguardo alla protezione dei dati personali».*

Infine, nel successivo Titolo II, dedicato all'Autorità di Controllo, là dove si delineano i compiti del Garante, è indicato all'art. 154-ter il potere di agire e di rappresentanza in giudizio stabilendo che *«1. Il Garante è legittimato ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali.2. Il Garante è rappresentato in giudizio dall'Avvocatura dello Stato, ai sensi dell'articolo 1 del regio decreto 30 ottobre 1933, n. 1611. 3. Nei casi di conflitto di interesse, il Garante, sentito l'Avvocato generale dello Stato,può stare in giudizio tramite propri funzionari iscritti nell'elenco».*

Parallelamente all'esercizio dei diritti dell'interessato di cui agli artt. da 15 a 22 del GDPR, spetta agli eredi la legittimazione ad agire per richiedere il risarcimento dei danni derivanti dalla violazione della normativa in materia di dati personali.

D: Quali sanzioni può infliggere il Garante per la protezione dei dati personali ai titolari del trattamento e ai responsabili del trattamento?

R: Il Garante, laddove rilevi il mancato rispetto delle disposizioni previste in materia di privacy, può infliggere sia ai titolari del trattamento che ai responsabili del trattamento delle sanzioni amministrative, ai sensi dell'art. 58 del Regolamento.

Più precisamente, il Garante può:

- rivolgere avvertimenti;
- ammonire l'avvocato, l'associazione o la società professionale;
- limitare temporaneamente o permanentemente un trattamento;

- sospendere i flussi di dati;
- ordinare di soddisfare richieste per l'esercizio dei diritti delle persone;
- ordinare la rettifica, limitazioni o cancellazione dei dati;
- ritirare la certificazione di conformità concessa all'avvocato, allo studio, all'associazione o alla società professionale, ovvero ordinarne il ritiro all'autorità di certificazione;
- comminare una sanzione amministrativa di importo compreso fra i 10 ed i 20 milioni di euro, ovvero, in caso di grandi studi internazionali, di importo compreso fra il 2% ed il 4% del fatturato mondiale.

D: Il Garante può adottare anche d'ufficio i provvedimenti di cui all'art. 58 del Regolamento?

R: Sì. Il Garante, all'esito dell'attività ispettiva della Guardia di finanza o in seguito ad una segnalazione (cfr. art. 144 Codice privacy), può adottare, anche d'ufficio uno dei provvedimenti di cui all'art. 58 del Regolamento.

L'art. 154 ter del Codice Privacy, nel delineare i compiti attribuiti al Garante, indica fra questi il potere di agire e di rappresentanza in giudizio, stabilendo che «1. *Il Garante è legittimato ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali.2. Il Garante è rappresentato in giudizio dall'Avvocatura dello Stato, ai sensi dell'articolo 1 del regio decreto 30 ottobre 1933, n. 1611. 3. Nei casi di conflitto di interesse, il Garante, sentito l'Avvocato generale dello Stato, può stare in giudizio tramite propri funzionari iscritti nell'elenco*».

D: Sono previste anche sanzioni penali?

R: Sì. L'art. 84 del Regolamento ha lasciato una certa discrezionalità ai singoli Stati, prevedendo quali limiti il rispetto del principio del ne bis in idem e dei criteri di effettività, proporzionalità e dissuasività. In Italia è stata prevista l'applicazione delle sanzioni penali per le fattispecie di reato di cui agli artt. 167, 167 bis, 167 ter, 168, 170 e 171 del Codice privacy.

In particolare, l'art. 168 del Codice privacy (Falsità nelle dichiarazioni al Garante) prevede quale sanzione la reclusione da sei mesi a tre anni per chiunque «*in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi*».

L'art. 170 del Codice privacy (Inosservanza di provvedimenti del Garante) prevede invece la reclusione da tre mesi a due anni per «*chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58,paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163*».