Ordine degli Avvocati di Genova
www.ordineavvocatigenova.it

Privacy per avvocati, alla luce delle modifiche introdotte dal GDPR

(aggiornamento con il d.lgs. 101/2018)

Consiglio dell'Ordine degli Avvocati di Genova

Relazionano

Avv. Cons. Alessandra Volpe

avv. Daniele Minotti - Foro di Genova

L'approccio corretto

Non dimentichiamoci di essere avvocati, dunque giuristi.

L'"allergia" alle leggi non ci appartiene, non ci deve appartenere, lasciamola ad altre categorie di "giuristi" o presunti (aspiranti) tali.

Basta documentarsi un po', senza panico, perché la riservatezza può anche essere un’opportunità, una valore da comunicare ai clienti.

Soprattutto…

"Leave no man behind"

Di cosa stiamo parlando?

Il 25 maggio 2018 è divenuto definitivamente applicabile (in tutti i Paesi UE) il Regolamento Generale sulla Protezione dei Dati Personali 2016/679, detto anche, dall'acronico inglese, GDPR.

Si tratta di un "adeguamento" rispetto alla precedente disciplina (il Codice d.lgs. 196/2013) e, trattandosi di Regolamento e non di Direttiva, è direttamente applicabile in tutti i Paesi UE.

Il 19 settembre 2018 è entrato in vigore il d.lgs. 101/2018 di adeguamento.

Testi e materiali sono accessibili dal sito del Garante Privacy, a partire dall'indirizzo

http://www.garanteprivacy.it/regolamentoue

Cambia qualcosa rispetto al passato?

SI'

In generale, nulla di rivoluzionario (nella maggioranza dei casi, specie nelle piccole realtà), ma qualcosa va fatto.

NON è vero che non si deve fare nulla

Le fonti

~~Legge 31 dicembre 1996, n. 675 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali~~

Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali (+ allegati) (come modificato dal d.lgs. 101/2018)

Regolamento europeo in materia di protezione dei dati personali 679/2016 (GDPR) + Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali (e alcuni allegati) + Decreto legislativo 10 agosto 2018, n. 101

I principi fondamentali

Articolo 1

Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle **persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2. Il presente regolamento protegge i **diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali**. (…)

(art. 8, par. 1, Carta diritti fondamentali UE e art. 16, par. 1, Trattato TFUE)

La Carta europea (2012/C 326/02)

Articolo 8 - Protezione dei dati di carattere personale

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

I principi fondamentali, ancora

Articolo 2

Ambito di applicazione materiale

1. Il presente regolamento si applica al **trattamento interamente o parzialmente automatizzato** di dati personali e al **trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi**.

Esenzioni (sempre art. 2)

2. Il presente regolamento non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Alcune definizioni (art. 4)

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

Alcune definizioni (art. 4)

2) «**trattamento**»: **qualsiasi operazione o insieme di operazioni**, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Alcune definizioni (art. 4)

7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

I principi del trattamento (art. 5 e C39)

- Liceità, correttezza, trasparenza
- Limitazione delle finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza
- Responsabilizzazione (rinvio)

La "responsabilizzazione" ("accountability"*)

Il titolare del trattamento è **competente per il rispetto del paragrafo 1** e **in grado di comprovarlo** («responsabilizzazione»)

(art. 5, comma 2 e C74)

Rappresenta la vera rivoluzione del GDPR, il cambiamento di rotta, l'opposta prospettiva.

Dal principio della responsabilizzazione discende tutto.

*) *Responsabilità incondizionata, formale o non, in capo a un soggetto o a un gruppo di soggetti (accountors), del risultato conseguito da un'organizzazione (privata o pubblica), sulla base delle proprie capacità, abilità ed etica. (fonte: Treccani online)*

La "liceità" del trattamento (art. 6)

- **Consenso per finalità**
- **Esecuzione contratto**
- **Obbligo di legge (del titolare)**
- Salvaguardia degli interessi vitali (interessato o altro)
- Interesse pubblico o connessione all'esercizio di pubblici poteri (titolare)
- Legittimo interesse (del titolare o di terzi - condizionato con altri legittimi interessi o libertà fondamentali)

Una prima conclusione

Si può, dunque, dire che, ordinariamente, la base delle liceità del trattamento da parte di un avvocato è rappresentata dall'*esecuzione del contratto* (il mandato), da alcuni *obblighi di legge* (es.: fiscali), chiaramente col limite dei dati necessari per detta esecuzione (i dati necessari per la "causa" e richiesti dalla legge e non di più).

E' difficile ipotizzare il trattamento di dati ulteriori, ma dobbiamo sapere che, se richiesti (ad esempio per una newsletter), il trattamento degli stessi sarà lecito soltanto con il consenso dell'interessato-cliente (persona fisica).

Sicché - fondamentale nella conclusione - di regola non occorre alcun consenso, ma, come vedremo, è sufficiente dare l'informativa.

Ma, allora, cosa dobbiamo fare?

Non esistono soluzioni precostituite e noi che siamo giuristi sappiamo quanto la legge debba essere interpretata e confrontata con il caso concreto.

Tuttavia, per le piccole realtà (che sono le più diffuse), tipo gli studi "unicellulari", con pochi collaboratori, anche i piccoli associati, ci sono pochi adempimenti.

Ma prima di vederli nel dettaglio…

…consapevolezza e responsabilizzazione…

Non possiamo fare finta di nulla. Un cliente si affida a noi, ci affida la sua vita, unitamente ai suoi dati di cui noi dobbiamo essere gelosi custodi per garantirne, anzitutto, integrità e riservatezza. Essere «avvocati», oggi, è anche questo.

Quante volte abbiamo sentito parlare di gravi incidenti sulle pratiche? Attacchi virus e malware, hard disk bruciati, perdita di chiavette, furti di supporti; banalmente, la perdita di un fascicolo cartaceo.

E’ accettabile che ciò succeda quando il rischio può, almeno, essere contenuto?

Consapevolezza dei rischi, responsabilizzazione nelle soluzioni.

Basta essere "avvocati"?

Art. 13 (Cod. Deont.) – Dovere di segretezza e riservatezza

L’avvocato è tenuto, nell’interesse del cliente e della parte assistita, alla rigorosa osservanza del segreto professionale e al massimo riserbo su fatti e circostanze in qualsiasi modo apprese nell’attività di rappresentanza e assistenza in giudizio, nonché nello svolgimento dell’attività di consulenza legale e di assistenza stragiudiziale e comunque per ragioni professionali.

(reprise) La Carta europea (2012/C 326/02)

Articolo 8 - Protezione dei dati di carattere personale

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

La tutela dei dati personali

- **Riservatezza**
- **Integrità**
- **Disponibilità**

Pertanto, non basta essere avvocati, non basta il rispetto del segreto, ma l'avvocato, in quanto titolare, deve proteggere i dati personali anche dalla distruzione o dalla perdita.

GLI ADEMPIMENTI IN PRATICA

L'informativa in generale

L'informativa era già prevista dal Codice (all'art. 13). Con il Regolamento (al corrispettivo art. 13) viene, in parte, semplificata, in parte "arricchita" per via di nuovi diritti introdotti dalla normativa europea.

Il titolare (l'avvocato) ha dei precisi obblighi fissati nell'art. 12 Regolamento

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma ***concisa****,* ***trasparente****,* ***intelligibile*** *e* ***facilmente accessibile****, con un* ***linguaggio semplice e chiaro****, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite* ***per iscritto*** *o con* ***altri mezzi****, anche, se del caso,* ***con mezzi elettronici****. Se richiesto dall'interessato, le informazioni possono essere fornite* ***oralmente****, purché sia comprovata con altri mezzi l'identità dell'interessato.*

L'informativa da vicino (art. 13 Reg.) 1/2

- Identità e recapiti titolare (indirizzo fisico, telefono, fax, email, ma si piò indicare anche soltanto quello fisico)

- ~~Contatti DPO (nuovo)~~

- Finalità e base giuridica

- ~~Legittimi interessi (nuovo)~~

- Eventuali destinatari

- ~~Trasferimenti estero (nuovo)~~

** Le voci barrate normalmente non si applicano alla piccole realtà.*

L'informativa da vicino (art. 13 Reg.) 2/2

- Periodo di conservazione o criteri utilizzati (almeno quello "fiscale")

- Info su diritto ad accesso, rettifica, cancellazione, limitazione, opposizione, portabilità (nuovo)

- Revocabilità consenso

- Info su reclamo a un'autorità di controllo (nuovo) (può essere sufficiente indicare il Garante italiano e l'indirizzo www.garanteprivacy.it)

- Obbligo legale o contrattuale oppure requisito necessario conclusione contratto

- Comunicazione (se) obbligatoria e conseguenze

- ~~Processo decisionale automatizzato, particolari e conseguenze profilazione (nuovo)~~

** Le voci barrate normalmente non si applicano alla piccole realtà.*

L'informativa quando e dove

Come abbiamo visto, di regola, non serve il consenso per trattare dati personali in esecuzione del mandato. Ma l'informativa serve sempre e deve essere resa **prima** di ottenere i dati.

Sul "**dove**" possiamo pensare a quattro soluzioni:

- Informativa esposta nei locali dello studio come se fossero condizioni generali del contratto (conosciute o conoscibili);
- Informativa riportata su un documento da far sottoscrivere (per la prova);
- Informativa incorporata nel mandato o nel preventivo (ma evitare di appesantire troppo il mandato);
- Informativa ("privacy policy") del sito dello studio e per i cookie (da aggiornare)

Ricordiamoci che l'informativa a norma GDPR è più ampia rispetto a quella precedente e deve essere più chiara e semplificata. Serve, pertanto, una revisione di quella precedente.

E i siti Internet? Informativa e cookie

Per l'informativa vale sempre l'art. 13, con i dovuti adattamenti

Per i cookie… > vedi Garante

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3585077

La revisione delle misure di sicurezza

Intanto, approfittiamo dell’occasione per fare un po’ di revisione della sicurezza, fisica e informatica, che serve ad evitare incidenti.

- Accessi limitati (porte, armadietti, "politica degli accessi" per collaboratori e dipendenti)
- Estintori
- Sicurezza informatica (la parola magica, spesso, è "aggiornamento")

Misure di sicurezza e GDPR: l'art. 32

«misure tecniche e organizzative adeguate»

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.

Chi si ricorda l'"allegato B" al Codice Privacy?

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557184

Informatiche

Sistema di autenticazione informatica

Sistema di autorizzazione

Altre misure di sicurezza

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

Misure di tutela e garanzia

Non informatiche

(L'Allegato B è stato abrogato, ma costituisce una buona base di partenza di materia, ovviamente con gli aggiornamenti tecnici del caso)

Il registro dei trattamenti: cos'è (art. 30 Reg.)

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.

Il contenuto del registro del titolare (art. 30, paragrafo 1):

- Nome e contatti titolare, responsabile, DPO
- Finalità del trattamento
- Descrizione interessati (es.: Colleghi, clienti e fornitori) e categorie di dati
- Destinatari della comunicazione (es. Colleghi e collaboratori)
- Trasferimento estero (di solito non applicabile alle piccole realtà)
- Termini per la cancellazione
- Descrizione misure di sicurezza tecniche e organizzative

Il registro dei trattamenti: perché

Il registro dei trattamenti non è sempre obbligatorio (v. art. 30, par. 5). Ma è consigliabile tenerlo, per diverse ragioni:

- attualmente, c'è una situazione di incertezza interpretativa e, onde evitare sanzioni (pesanti) si consiglia di tenerlo;
- d'altro canto, si tratta di un adempimento realmente elementare ed economico, da predisporre quasi "una volta per tutte";
- tenere un registro, aiuta la "responsabilizzazione" e può essere una buona presentazione in caso di accertamenti.

Il registro può essere cartaceo o elettronico (art. 30, par. 3).

Il responsabile "esterno" (art. 28)

1. Qualora un trattamento debba essere effettuato ***per conto del titolare del trattamento****, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.*

La nomina è su base contrattuale.

Esempi: fornitore di tecnologia informatica che mantiene i nostri server in "housing".

ATTENZIONE: è possibile che un avvocato (o uno studio associato) sia individuato come responsabile dai clienti.

"Incaricati" e "autorizzati al trattamento"

La prima è una figura prevista esclusivamente nel Codice italiano, non nel Regolamento europeo che preferisce parlare di "autorizzati al trattamento". Dunque, in qualche modo occorre tenerne conto.

Si tratta, molto semplicemente, di collaboratori e dipendenti che, appunto, sono da noi autorizzati e posti sotto la nostra diretta autorità.

E' sufficiente, come in passato, una lettera di attribuzione di incarico che precisi informazioni e istruzioni.

Siccome le norme europee non sono intervenute sul punto, bastano i modelli precedentemente utilizzati.

Codici di condotta e certificazioni

Non garantiscono esenzioni di responsabilità, ma costituiscono "presunzione" di messa a norma…

L'avvocatura conosce già il "Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive" (Allegato A.6 del Codice)

Naturalmente, i codici di condotta (artt. 40 e 41 Reg.) devono essere approvati dal Garante, mentre le certificazioni (artt. 42 e 43 Reg.) devono essere rilasciate da soggetti accreditati (dal Garante o da apposito organismo accreditato).

Ricapitolando

- Consapevolezza e responsabilizzazione
- Revisione sicurezza e misure
- Revisione informativa
- Predisposizione del registro (consigliato, non sempre obbligatorio)
- Nomina responsabili esterni (se richiesto)
- Nomina autorizzati al trattamento
- Certificazioni e/o codici di condotta

e… violazione dei dati (data breach)… segue…

La violazione dei dati (data breach)

"*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*" (art. 4 n. 12 Reg.)

Banalmente, potrebbe essere un incidente informatico che rende irrecuperabili i dati oppure un accesso abusivo ovvero la "perdita" di un cartaceo.

La violazione dei dati (data breach): che fare?

Il codice prevede due obblighi:

- **Notifica al Garante** "a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" (art. 33)
- **Comunicazione agli interessati** (art. 34) qualora sussista un "rischio elevato per i diritti e le libertà delle persone fisiche" e con alcune eccezioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e 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;

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 di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Attenzione alle sanzioni

Artt. 83 e 84 Regolamento

Art. 166 Codice

Ipotesi di sanzioni penali

Artt. 167 e ss. Codice

Altre ed eventuali

C'è altro da fare nelle piccole realtà?

- Valutazione d'impatto sulla protezione dei dati (art. 35) - NO
- Consultazione preventiva (art. 36) - NO
- DPO (Data Protection Officer - Responsabile della protezione dei dati RDP) (art. 37-39) - NO

Contatti

Daniele Minotti
daniele@minotti.net

MATERIALI ESTERNI

CNF

http://www.consiglionazionaleforense.it/web/cnf/-/gdpr-linee-guida-avvocati

Unione Triveneta

http://www.avvocatitriveneto.it/vademecum-privacy-unione-triveneta-2018/

BARI

http://www.ordineavvocati.bari.it/default.asp?idlingua=1&idContenuto=5112&page=GDPR+per+studi+legali

GARANTE

https://www.garanteprivacy.it/regolamentoue

Avv. Massimiliano Nicotra

http://www.avvmax.com/registro