REGOLAMENTO GENERALE IN TEMA DI PRIVACY:

OBBLIGHI (MINIMI?) PER GLI AVVOCATI

a cura di Gianluca Gambogi

Sommario: **1)** Applicabilità del Regolamento [U.E.] 2016/679 alla professione di avvocato – **2)** I limiti, importanti, riferibili alla professione forense - **3)** I dati personali riguardanti terzi - **4)** Che cosa si intende per dato personale? - **5)** Il concetto di trattamento del dato - **6)** Il rapporto, delicato, tra trattamento e consenso - **7)** Gli adempimenti obbligatori dell'avvocato: l'informativa, il registro delle attività di trattamento, la protezione del dato – **8)** Attività di controllo e sanzioni per la violazione

* * *

1) <u>Applicabilità del Regolamento [U.E.] 2016/679 alla professione di avvocato</u>

Come noto il Regolamento [U.E.] n. 2016/679 del Parlamento europeo del 27 aprile 2016 è applicabile, in via diretta, a tutti i paesi dell'Unione a partire dal 25 maggio 2018.

Il Regolamento (che prevede ben 173 *considerando* e cioè premesse) è suddiviso in 11 capi:

- il capo I (artt. 1-4) contiene le disposizioni generali;
- il capo II (artt. 5-11) i principi;
- il capo III, suddiviso in 5 sezioni (artt. 12-23) riguarda i diritti dell'interessato;
- il capo IV, suddiviso in 5 sezioni (artt. 24-43), attiene al titolare del trattamento e responsabile del trattamento;
- il capo V (artt. 44-50) detta disposizioni in tema di trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;
- il capo VI, suddiviso in 2 sezioni (artt. 51-59), riguarda le autorità di controllo indipendenti;

- il capo VII, suddiviso in 3 sezioni (artt. 60-76), concerne la cooperazione e coerenza;
- il capo VIII (artt. 77-84) riguarda i mezzi di ricorso, le responsabilità e le sanzioni;
- il capo IX (artt. 85-91) le disposizioni relative a specifiche situazioni di trattamento;
- il capo X (artt. 92 e 93) gli atti delegati e gli atti di esecuzione;
- il capo XI (artt. 94-99) le disposizioni finali.

Solo una parte (minima) delle suddette disposizioni riguarda l'avvocato in quanto professionista.

Tuttavia è necessario evidenziare che, al momento, non è stato emanato il provvedimento delegato al Governo con il quale stabilire la compatibilità del Codice della privacy del 2003 con la nuova normativa.

Un'opera di coordinamento importante, quella di cui sopra, poiché alcune norme del Codice sono compatibili e perfettamente in linea con quelle del Regolamento europeo, mentre altre sono obiettivamente non più compatibili.

Inoltre occorrerà comunque attendere i chiarimenti del Garante sui principali adempimenti che il singolo avvocato dovrà osservare posto che i chiarimenti precedenti, soprattutto quelli del 3 giugno 2004, si riferivano al Codice della privacy e quindi dovranno essere rivisti e implementati.

Appare tuttavia condivisibile l'orientamento in forza del quale il Regolamento europeo è, in via generale, sostanzialmente finalizzato a disciplinare le modalità di trattamento dei dati personali delle persone fisiche sotto un duplice profilo:

- quello dell'informativa e del consenso nella loro acquisizione;
- quello dell'utilizzo (legittimo) e la circolazione (altrettanto legittima) dei dati.

Ciò trova conferma nel diritto soggettivo dell'individuo di disporre dei propri dati, quali aspetti ricollegabili al fondamentale diritto di identità e personalità, nonché sul fatto che il titolare del trattamento viene ad assumersi la responsabilità (*accountability*) del trattamento di tali dati e pertanto deve adottare tutte quelle misure necessarie alla *protezione* del dato stesso.

2) <u>I limiti, importanti, riferibili alla professione forense</u>

Come detto in precedenza l'avvocato è soggetto, sia pure ad una parte (minima) delle disposizioni regolamentari, allorquando tratta i dati personali del proprio cliente.

Vale la pena di ricordare che il trattamento del dato è senz'altro consentito (art. 9, comma 2, lett. f del nuovo Regolamento) **per accertare, esercitare o**

difendere un diritto in sede giudiziaria o ogni qualvolta le autorità giurisdizionali esercitino le loro funzioni.
Senza dimenticare che il *considerando* n. 52, cioè la premessa n. 52 del Regolamento, **estende il principio** di cui sopra anche **alla sede amministrativa** (e quindi ai ricorsi gerarchici e alle difese dinanzi agli organi di disciplina) **o stragiudiziale**.
Ne consegue quindi che un avvocato può sempre trattare un dato personale per esercitare la difesa di un diritto in qualunque sede si trovi a farlo.
Ciò significa anche che tale trattamento, poiché consentito da una norma giuridica, è legittimo a prescindere dal consenso dell'interessato, da considerarsi implicito e contestuale all'affidamento dell'incarico.
Peraltro laddove nell'esame della posizione del cliente quest'ultimo riferisse informazioni personali riguardanti, ad esempio, il suo stato di salute, la religione di appartenenza, l'orientamento politico, le abitudini sessuali ed espressamente negasse il consenso all'utilizzo di tali informazioni, è evidente che l'avvocato non potrebbe utilizzarle in ambito difensivo ed in ogni caso non potrebbe rivelarle e ciò a prescindere dalla normativa sulla privacy di cui trattasi: prova ne sia che l'art. 6 della nuova legge professionale, n. 247/2012, impone all'avvocato una rigorosa osservanza del segreto professionale **e del massimo riserbo sui fatti e sulle circostanze apprese nell'attività di rappresentanza e assistenza**.
Senza considerare che il dovere di segretezza e riservatezza trova conferma nell'art. 13 del nuovo Codice Deontologico Forense che sostanzialmente ribadisce il principio indicato dalla legge professionale.
Infine non può dimenticarsi che laddove l'avvocato dovesse rivelare, senza giusta causa, un dato (e quindi una notizia) a lui riferita dal cliente, commetterebbe il reato previsto e punito dall'art. 622 del codice penale, norma quest'ultima che si riferisce ad ogni notizia (e quindi anche a quelle afferenti la personalità del cliente) appresa in ragione del rapporto professionale.

3) <u>I dati personali riguardanti terzi</u>
E' peraltro possibile che il cliente riferisca all'avvocato dati personali di terzi soggetti e, ovviamente, anche della controparte.
Nel caso in cui, ad esempio, all'avvocato venga chiesto di procedere ad una separazione giudiziale con richiesta di addebito nei confronti dell'altro coniuge è possibile che vengano riferiti dati personali riguardanti le relazioni (e quindi soggetti terzi) intrattenute dalla controparte.

Ovvio che tali notizie sono comunque coperte dal segreto professionale e l'avvocato non potrà mai divulgarle: laddove lo facesse, come abbiam visto in precedenza, violerebbe la legge professionale, il Codice Deontologico e soprattutto commetterebbe un reato laddove ricorrano gli elementi costitutivi della norma incriminatrice di cui all'art. 622 c.p.

Potrà invece avvalersi di tali notizie, sempre che non siano state illecitamente raccolte come ribadito recentemente dalla Suprema Corte (Sezione VI Civile, 8 novembre 2016, n. 22677), nell'ambito della tutela giudiziaria che dovrà garantire al proprio assistito con il limite, insuperabile, di indicare notizie o circostanze strettamente connesse e pertinenti all'oggetto del giudizio.

Quanto al profilo dell'acquisizione illecita è vero infatti che con la citata sentenza la Suprema Corte di Cassazione, pur non essendo presente nel codice di procedura civile una norma analoga all'art. 191 del codice di procedura penale, ha stabilito che: "non è utilizzabile nel giudizio civile il materiale probatorio raccolto illegittimamente" (fattispecie riferibile ad un giudizio di separazione personale tra coniugi e avente ad oggetto la sottrazione fraudolenta di files audio).

D'altra parte l'acquisizione di notizie riguardanti terze persone può tranquillamente verificarsi anche nell'ambito della difesa penalistica.

Si pensi, ad esempio, alle investigazioni difensive di cui all'art. 391-*bis* e segg. del codice di procedura penale.

Problema quest'ultimo già affrontato in passato, dallo stesso Garante della privacy, e risolto nel senso di consentire appieno il diritto di difesa non solo durante lo svolgimento di un giudizio necessariamente già instaurato, ma anche nella fase antecedente, come quella delle investigazioni difensive, laddove vi sia correlazione tra attività difensiva e successiva attività processuale: ovvio che nel caso di specie l'attività dell'indagine difensiva deve quindi assumere il carattere di fase propedeutica al futuro giudizio.

Prova ne sia che l'art. 391-*nonies* del codice di procedura penale prevede e disciplina proprio l'attività investigativa preventiva che può essere svolta dal difensore, appositamente nominato, anche per la sola eventualità che si instauri un procedimento futuro.

E' pertanto più che probabile che nel corso di queste attività vengano acquisiti dati personali riguardanti terzi, ma vale, come sempre, il principio dell'utilizzabilità solo ed esclusivamente per quei dati strettamente connessi ed oggettivamente riferibili al procedimento penale in corso o a quello che verrà.

4) <u>Che cosa si intende per dato personale?</u>

L'art. 4 del Regolamento europeo, secondo una buona tecnica normativa, disciplina tutte le definizioni nell'evidente tentativo di eliminare, il più possibile, incertezze interpretative.

Tra le varie definizioni si rinviene, al n. 1, proprio quella di dato personale.

Si considera tale **qualsiasi informazione riguardante una persona fisica identificata o identificabile e si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on-line, o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.**

E' evidente che la definizione di 'dato personale' è in perfetta continuità con la direttiva europea n. 95/46 ed anche con il codice della privacy del 2003.

Quindi gli elementi caratterizzanti il dato personale sono: l'informazione, la persona fisica (il soggetto a cui il contenuto dell'informazione viene ricollegato), l'identificazione o l'identificabilità, uno o più elementi caratteristici che contraddistinguono l'informazione (identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale).

Come già riferito in precedenza, a prescindere dal Regolamento europeo, l'avvocato non può rivelare un dato personale acquisito nel corso dei colloqui con il cliente e ciò si riferisce, in particolare, proprio a quei dati non rilevanti ai fini specifici della difesa richiesta.

5) <u>Il concetto di trattamento del dato</u>

Per **trattamento del dato** si intende, a norma dell'art. 4, n. 2: *"Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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, la distruzione".*

Anche in questo caso nessuna novità e nessuna sorpresa poiché si tratta di una disposizione che si pone in continuità sia con la direttiva europea n. 95/46.

Per trattamento quindi si intende, almeno stando alla descrizione contenuta nelle disposizioni (vecchia e nuova), l'attività posta in essere dal soggetto che tratta, cioè utilizza o impiega, il dato personale già raccolto.

6) <u>Il rapporto, delicato, tra trattamento e consenso</u>

E' di tutta evidenza che, **fermo restando quanto rilevato in precedenza per la professione di avvocato nella quale non vi è necessità del consenso,** in assenza di quest'ultimo, il trattamento dei dati personali da parte di soggetti diversi dai legali difensori non potrà avvenire.

Senza entrare, poiché sostanzialmente non interessa ai fini della presente nota, nell'esame circa la natura del soggetto titolare del trattamento e cioè se sia da considerarsi privato oppure pubblico (distinzione che peraltro appare priva di considerazione anche da parte del legislatore europeo che non distingue tra condizione applicabile a privati e a pubblici soggetti salvo evidenziare che il trattamento da parte degli organi uffici e agenzie dell'Unione è regolato da altro Regolamento europeo), **è assai più importante sottolineare che, come già riferito in precedenza, chi tratta il dato deve farlo con assunzione di responsabilità (*accountability*)**.

Il principio di responsabilità è riferibile a due distinte fasi: ricevere il consenso dell'interessato e, successivamente, proteggere i dati acquisiti.

Prima di ogni altra cosa quindi si deve ottenere il consenso dell'interessato che deve essere **libero, non equivoco e specifico** non essendo sufficiente un consenso meramente generico.

E' necessaria la forma scritta per il consenso?

In realtà tale forma non è prevista obbligatoriamente dalla normativa in vigore (tra pochi giorni) e **pertanto si deve ritenere valido anche il consenso orale.**

Prova ne sia che l'art. 4, n. 11, che definisce il consenso, fa riferimento a qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale lo stesso manifesta il proprio assenso mediante dichiarazione o azione positiva inequivocabile e quindi anche al cosiddetto 'fatto concludente'.

E' possibile peraltro che l'avvocato, pur non avendo necessità di ottenere un consenso chieda, ai fini probatori, la sottoscrizione di una scrittura privata del soggetto legittimato a prestarlo.

Tale scrittura privata avrà quantomeno un valore indiziario e comunque, a meno del disconoscimento della firma, si riterrà proveniente dall'interessato.

Per quanto attiene invece alle modalità di protezione del dato acquisito (cioè l'altro versante rispetto al quale si valuta il principio di responsabilità) si deve far riferimento, prima di ogni altra cosa, alla messa in sicurezza dei dati personali acquisiti attraverso misure tecniche organizzative che, ai sensi

dell'art. 24 del Regolamento, siano adeguate a garantire la conformità alle previsioni del Regolamento stesso.
Peraltro proprio l'art. 24 pone l'obbligo di riesaminare ed aggiornare le misure di sicurezza di protezione del dato laddove necessario.
Ovvio che tali misure riguardano anche la tenuta dell'archivio (informatico) ed altre specifiche condotte richiamate dall'art. 32, quali, ad esempio:
a) la pseudonimizzazione e la cifratura dei dati personali (che non pare applicabile agli avvocati);
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.
E' peraltro ragionevole dubitare che le disposizioni contenute nell'art. 24, stante anche il richiamo agli artt. 40 e 42 del Regolamento, siano direttamente applicabili ai professionisti e, in particolare, agli avvocati.

7) Gli adempimenti obbligatori dell'avvocato: l'informativa, il registro delle attività di trattamento, la protezione del dato

Alla luce di quanto sopra riferito è bene ricordare che uno strumento ancor oggi utile per consentire all'avvocato di valutare *l'impatto* della normativa è rappresentato dal già richiamato documento denominato *Chiarimenti sui principali adempimenti in materia di protezione di dati personali nello svolgimento dell'attività forense* (*doc.webn1007280*), del 3 giugno 2004, inviato dall'allora Segretario generale del Garante della privacy (oggi Garante europeo della privacy) al Consiglio Nazionale Forense.
La lettura di tale documento, pur risalente nel tempo, consente ancor oggi di poter arrivare alla ragionevole conclusione che l'avvocato può assolvere agli obblighi di cui trattasi con **modalità semplificate**.
In ragione di queste ultime vale la pena di ricordare innanzi tutto che l'avvocato non è obbligato ad indicare un **responsabile** del trattamento e d'altra parte la lettura stessa consente di ritenere che la maggior parte dei trattamenti di dati effettuati nell'esercizio dell'attività forense non è neppure soggetta a notificazione.
In ragione di quanto sopra il Consiglio dell'Ordine, alla luce anche delle recenti linee guida del C.N.F., alle quali espressamente si rinvia, ritiene di

suggerire ai propri iscritti il rispetto di tre precisi adempimenti e cioè quelli riguardanti:

a) **l'informativa [è sufficiente anche quella orale]**;

b) **il registro di trattamento**;

c) **la protezione del dato**.

* * *

Per quanto attiene all'**informativa** (onere senz'altro obbligatorio per l'avvocato) giova osservare che vi è perfetta continuità normativa tra gli artt. 13 e 14 del nuovo Regolamento europeo e il Codice della privacy vigente.

La suddetta, è bene ricordarlo, **può essere fornita anche oralmente in quanto non è previsto un obbligo per l'avvocato di inviare al cliente una informativa scritta.**

Prova ne sia che, stando al citato provvedimento del Garante della privacy, è senz'altro possibile utilizzare formule colloquiali per evidenziare, anche in modo sintetico, ma senza lacune, le circostanze che riguardano **finalità e modalità del trattamento.**

Quindi, in buona sostanza, l'avvocato dovrà informare il cliente, oralmente o per iscritto, sulle seguenti questioni:

- *finalità del trattamento* (chiaramente per l'avvocato il trattamento dei dati è finalizzato all'utilizzo in ambito giudiziale o extragiudiziale);
- *modalità del trattamento* (e quindi occorrerà segnalare se si realizza attraverso operazioni con o senza l'ausilio di strumenti elettronici);
- *effetti del rifiuto di fornire i dati* (ovvio che il mancato conferimento di alcuni dati personali impedisce automaticamente lo svolgimento dell'attività difensiva in qualunque sede sia essa richiesta).
- *finalità della comunicazione dei dati* (finalità che per l'avvocato riguarda lo svolgimento dell'incarico difensivo);
- *trasferimento (eventuale) dei dati all'estero* (per l'avvocato tale eventualità si presenterà solo nell'ambito dell'esercizio di attività difensive che si svolgono presso autorità giudiziarie sovranazionali o estere);
- *durata della conservazione* (i dati sono conservati per il periodo necessario all'espletamento dell'attività e comunque per un periodo non superiore a 10 anni dalla conclusione della stessa);
- *titolare del trattamento;*
- *i diritti dell'interessato* (rettifica, cancellazione, limitazione, opposizione e perfino revoca del consenso anche se, come visto in precedenza, quest'ultimo non pare necessario per l'esercizio delle attività forensi).

E' da notare infine che, stando alla normativa europea, oltre alla informativa diretta (o più precisamente primaria dal punto di vista della tempistica) esiste persino l'obbligo di informativa successiva laddove si

verifichi un ulteriore e diverso trattamento riferibile ad un altro e diverso incarico professionale (nel caso del difensore, quindi, la suddetta ipotesi potrà, semmai, verificarsi laddove la stessa persona affidi, successivamente, un diverso mandato difensivo per altra questione).

* * *

Il **registro concernente le attività di trattamento**, previsto dagli artt. 30 e 32 del Regolamento europeo, **è seriamente dubitabile** che debba essere obbligatoriamente istituito dall'avvocato.

Prova ne sia che **l'art. 30, comma 5, del Regolamento europeo prevede che tale obbligo non sussista per le imprese o organizzazioni con meno di 250 dipendenti, a meno che non si effettui il trattamento di dati particolari e cioè quelli sensibili e biometrici previsti dall'art. 9 dello stesso Regolamento**.

Ma come abbiamo già visto in precedenza non v'è dubbio che questi ultimi dati siano sempre trattati dall'avvocato nell'ambito delle attività forensi e come tali, in virtù dell'art. 9, comma 2, lett. f, non soggetti ad alcun obbligo di preventivo consenso: non si comprende quindi perché in virtù di tale regime di trattamento per l'avvocato, quest'ultimo debba tenere il registro di cui trattasi.

Si tratta, più precisamente, di dati (che rivelano l'origine raziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o anche all'orientamento sessuale) per i quali l'avvocato non ha alcuna necessità di consenso per il trattamento tenuto conto che utilizzerà i medesimi per accertare, esercitare o difendere un diritto in sede giudiziaria ed abbiamo visto che, grazie alle premesse del Regolamento europeo, ciò vale anche per la fase giudiziale e per le difese in sede amministrativa.

Perché mai quindi un legale dovrebbe farsi carico dell'istituzione di un registro del trattamento?

Come potrebbe infatti giustificarsi, laddove si ammettesse l'obbligo di cui sopra per l'avvocato, un così marcato *disallineamento* rispetto ai principi desumibili dal Regolamento europeo che, come detto, prevede tale registro per enti con più di 250 dipendenti.

Ciò conferma che il fine delle disposizioni riguardanti il registro delle attività di trattamento è quello di garantire la privacy dei cittadini rispetto a soggetti che trattano dati **su larga scala**.

Per convincersi di ciò è sufficiente analizzare con attenzione le disposizioni contenute proprio nell'art. 30, comma 1, lett. a-b-c-d-e-f-g.

Nonostante tali considerazioni che appaiono meritevoli di attenta valutazione anche da parte del Garante (che confidiamo possa fornire precise indicazioni

di conferma), stante l'intervenuto orientamento del C.N.F., che considera obbligatorio il registro di cui trattasi, è necessario, per ragioni di prudenza e di attenzione nei confronti dei Colleghi tutti, invitare all'istituzione del registro secondo il modello predisposto proprio dal C.N.F.

* * *

Per quanto attiene infine alla **protezione dei dati**, tenuto conto che in pratica in qualsiasi studio legale, dai più significativi a quelli di recente apertura (quindi con realtà organizzative assai più semplici), la stessa avviene mediante strumenti informatici e non più cartacei, è opportuno che l'avvocato si premuri di installare un sistema tale da garantire misure tecniche idonee alla protezione stessa.

D'altra parte, così come correttamente hanno valutato i primi commentatori della normativa europea, la sicurezza del trattamento prevista dall'art. 32 offre solo alcune novità rispetto a quanto gli avvocati italiani ben conoscono: prova ne sia che le misure minime di sicurezza sono già chiaramente indicate nel Codice della privacy italiano (artt. 33 e segg.) e soprattutto l'allegato B).

D'altronde, proprio nell'allegato B), si fa riferimento, in maniera specifica, al cosiddetto *dato sensibile o giudiziario* ribadendo che questa tipologia di dati sono protetti, contro l'accesso abusivo, proprio dall'art. 615-*ter* del codice penale.

Difficile pensare che la normativa europea abbia quindi abrogato le norme del nostro Codice della privacy in tema di sicurezza (anche se, come noto, siamo ancora in attesa del decreto legislativo che dovrà *armonizzare* i principi normativi italiani a quelli sovranazionali) poiché non appaiono certo incompatibili e comunque in grado di garantire un puntuale riferimento per adeguarsi al dovere di protezione.

A tal proposito giova infine notare come un qualsiasi programma cosiddetto di 'protezione antivirus', reperibile sul mercato, offre garanzie di adeguata protezione che sono ad un livello più che sufficiente di tutela degli interessati: basterà quindi che gli avvocati si dotino di tale programma, come certamente si saranno già dotati da molti anni.

Semmai appare tuttavia opportuno suggerire di verificare e riesaminare i rapporti contrattuali in essere con i fornitori del programma per verificare eventuali *falle* rispetto magari a programmi più aggiornati nel frattempo usciti sul mercato.

Infine è bene ricordare che, come si è più precisamente evidenziato in precedenza, l'informativa, sia pur orale, deve fornire al cliente anche i ragguagli sulla protezione dei dati che lo studio legale offre attraverso gli strumenti informatici utilizzati in quel preciso periodo.

8) <u>Attività di controllo e sanzioni per la violazione</u>

Il nuovo Regolamento europeo prevede la possibilità di infliggere, per le violazioni accertate, sia sanzioni amministrative pecuniarie (previste dall'art. 83), sia la possibilità (in forza della premessa 149, per gli Stati membri) di sanzioni penali a condizione che non si pongano in contrasto con il principio del *ne bis in idem* quale interpretato dalla Corte di Giustizia Europea.

Dal tenore delle somme indicate come sanzione amministrativa pecuniaria emerge un'ulteriore conferma e cioè che le medesima valgano, principalmente, per soggetti completamente diversi dal professionista avvocato.

Le sanzioni non potranno prescindere comunque dalla considerazione di alcuni elementi quali la gravità e la durata della violazione, il carattere doloso/colposo della stessa, le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dall'interessato, il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi.

E' bene tuttavia ricordare che nel Codice della privacy del 2003 (D.Lgs. n. 196) sono previste sia sanzioni amministrative, che illeciti penali.

Nel Regolamento si fa riferimento in senso generale alle autorità di controllo oltre che europee, anche dei singoli Stati membri.

Ciò significa, in altre parole, che appare corretto l'orientamento secondo il quale l'autorità di controllo nazionale italiano è il Garante della privacy.

<u>Si allegano i seguenti modelli</u>:

1) informativa [che è bene ricordare può essere anche orale];

2) registro trattamento dei dati, così come predisposto dal C.N.F. [che è bene ricordare non è da considerarsi obbligatorio]