CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

NORMATIVA ANTIRICICLAGGIO E PRIVACY

Il d.lgs. n. 231 del 2007 alla luce del GDPR

Dott. Andrea Di Gialluca

Roma, 18 febbraio 2019

Studio Visentini, Marchetti e Associati

VISENTINI MARCHETTI E ASSOCIATI

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Sommario

1. *Normativa sulla privacy. Cenni sugli aspetti operativi per gli studi professionali*

2. *Normativa sulla privacy e normativa antiriciclaggio*

1. NORMATIVA SULLA *PRIVACY*. ASPETTI OPERATIVI PER GLI STUDI PROFESSIONALI.

CENNI

Privacy: quadro normativo e di prassi di riferimento

Normativa europea:
- Artt. 7 e 8, Carta dei diritti fondamentali dell'Unione Europea;
- Art. 16 TFUE;
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio adottato il 27 aprile 2016 (GDPR).

Normativa interna:
- D.Lgs. n. 196 del 30 giugno 2003 («Codice della *Privacy*»);
- Art. 13, legge 25 ottobre 2017, n. 163 («*Legge di delegazione europea 2016-2017*»);
- Art. 28, legge 20 novembre 2017, n. 167 («*Legge Europea 2017*»);
- Art. 1, commi 1020-1025, legge 27 dicembre 2017, n. 205 («*Legge di Bilancio 2018*»);
- Schema di decreto legislativo A.G. n. 22.

Prassi europea ed interna:
- Linee Guida del Gruppo di Lavoro *ex* art. 29, WP29, ora *European Data Protection Board;*
- Documenti Garante della *Privacy*;

Regolamento (UE) 2016/679 del 27 aprile 2016 (GDPR).

- Applicazione diretta a partire dal 25 maggio 2018 in tutti i Paesi facenti parte dell'Unione Europea; → Abrogazione della previgente normativa privacy europea contenuta nella Direttiva 95/46/CE (dalla quale ha avuto origine anche il Codice della *Privacy* italiano)

- Soggetti tutelati: persone fisiche → non si applica alle persone giuridiche (salvo, ad esempio, con riguardo ai dati personali del legale rappresentante, persona fisica).

- Soggetti obbligati → «**Impresa**» con ciò intendendosi (art. 4, GPDR) «*la persona fisica o giuridica,* ***indipendentemente dalla forma giuridica rivestita****, che eserciti* ***un'attività economica****, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica*». –> Sono ricompresi i professionisti

- Ambito territoriale: trattamenti effettuati:

- dai titolari del trattamento e dai responsabili del trattamento stabiliti nel territorio UE in base al «principio di stabilimento»;
- secondo il luogo in cui si trovano i soggetti interessati dal trattamento.

L'art. 13 della legge n. 163 del 2017 ha delegato il governo ad effettuare il **coordinamento** tra la normativa europea, direttamente applicabile nell'ordinamento dal 25 agosto 2018, e quella nazionale

È stato pubblicato sulla Gazzetta Ufficiale n. 205 del 4 settembre 2018 il **d.lgs. 10 agosto 2018, n. 101,** recante disposizioni per **l'adeguamento della normativa nazionale alle disposizioni del GDPR.**

Pertanto, attualmente, **convivono due diverse e principali discipline con riguardo alla *Privacy*** (cui si aggiungono, ulteriori normative, come quella relativa alla c.d. *e-privacy,* attualmente in corso di revisione, il d.lgs. 18 maggio 2018, n. 51, attuativo della Direttiva UE 2016/680 e la Direttiva UE 2016/681):

- da un lato, la normativa europea **(GDPR);** e

- dall'altro, la normativa nazionale, quale **il Codice della *Privacy*, come modificato dal suddetto d.lgs. 101 del 2018.**

I **soggetti che «ruotano» attorno alla normativa *privacy*** sono i seguenti:

1. *«**Interessato**»;*
2. *«**Titolare del trattamento**»;*
3. *«Contitolare del trattamento»;*
4. *«Destinatario» e «terzo»;*
5. *«Designato o autorizzato »;*
6. *«**Responsabile del trattamento**»;*
7. *«Sub-responsabile del trattamento»;*
8. *«Rappresentante»;*
9. *«Data protection officer (DPO o RPD).*

I **diritti degli interessati** sono disciplinati dal Capo III del GDPR rubricato "diritti degli interessati", suddiviso in cinque sezioni, negli artt. da 12 a 23. Si tratta, in particolare, dei seguenti diritti:

a) diritto di accesso ai dati personali;
b) diritto di rettifica e di integrazione;
c) diritto di cancellazione/diritto all'oblio;
d) diritto di opposizione;
e) diritto di revocare il consenso;
f) diritto alla limitazione di trattamento;
g) diritto alla portabilità dei dati;
h) diritto a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato di dati.

I **principi sui quali si fonda il GDPR** sono i seguenti:

- Il principio di proporzionalità e del bilanciamento di interessi;
- Il principio di liceità, correttezza e trasparenza;
- Il principio di limitazione della finalità;
- Il principio di minimizzazione dei dati;
- Il principio di limitazione della conservazione;
- Il principio di esattezza;
- Il principio di integrità e riservatezza;
- Il principio della neutralità tecnologica;
- Il principio di accountability;
- I principi di "privacy by design" e di " privacy by default";
- Il principio di ragionevolezza;
- Il principio del rischio inerente al trattamento.

Base giuridica del trattamento (*art. 6 GDPR*) → Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il **consenso al trattamento dei propri dati personali** per una o più specifiche finalità;

b) il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la **salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;**

e) il trattamento è necessario per **l'esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento o di terzi** (ad alcune condizioni).

Check list «documentale» Privacy alla luce del GDPR e del nuovo Codice *Privacy*		
Adempimento	**Breve descrizione**	**Riferimento normativo**
Registro delle attività di trattamento	In esso devono essere indicate le tipologie di informazioni da registrare sia per il titolare del trattamento che per il responsabile del trattamento. E' obbligatorio in alcuni casi (quando il trattamento dati potrebbe comportare un rischio per i diritti e le libertà degli interessati; quando il trattamento dati non è occasionale; quando i trattamento dati è effettuato su categorie particolari di dati *ex* art. 9 GDPR e 10 GDPR).	*Art. 30 GDPR Gruppo di Lavoro WP29*
Informativa da rilasciare all'interessato	Deve essere rilasciato all'interessato apposita informativa all'atto del conferimento dell'incarico professionale	*Art. 13 GDPR*
Verifica base giuridica / consenso da parte dell'interessato	Occorre verificare la presenza di una base giuridica che legittimi il trattamento dei dati personali (es. Contratto, Consenso, Interesse legittimo, obbligo di legge), comuni e particolari (ex artt. 9 e 10 GDPR). Il consenso deve essere rilasciato dall'interessato all'atto del conferimento dell'incarico.	*Artt. 7, 8 e 9 GDPR*

Check list «documentale» Privacy alla luce del GDPR e del nuovo Codice *Privacy*

Adempimento	Breve descrizione	Riferimento normativo
Lettere incarico nei confronti degli Incaricati del Trattamento	II titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.	*Artt. 4, n. 10, 28, par. 3, lett. b), 29 e 32, par. 4 del GDPR,; l'art. 2-quaterdecies Codice Privacy*
Lettere incarico nei confronti dei Responsabili del Trattamento	I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento	*Art. 28 GDPR*
Lettera incarico Responsabile per la Protezione dei Dat	Il GDPR affida al DPO, fra gli altri, il compito di sorvegliare l'osservanza del Regolamento stesso, assistendo il Titolare e/o il Responsabile del Trattamento. E' obbligatorio in alcuni casi (autorità pubbliche; monitoraggio regolare e sistematico degli	*Art. 37 GDPR*

(Continua nella slide successiva…)

Check list «documentale» Privacy alla luce del GDPR e del nuovo Codice *Privacy*		
Adempimento	**Breve descrizione**	**Riferimento normativo**
Modulo per l'esercizio dei diritti dell'interessato	Il titolare del trattamento deve assicurare che l'interessato possa agevolmente esercitare i propri diritti (diritto di accesso ai dati personali; diritto di rettifica e di integrazione; diritto di cancellazione e il c.d. "diritto all'oblio"; diritto di opposizione; diritto di revocare il consenso; diritto alla limitazione di trattamento; diritto alla portabilità dei dati; diritto a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato di dati).	*Artt. 12, 15, 16, 17, 18, 20, 21 GDPR*
Valutazione d'impatto (DPIA)	La valutazione di impatto sulla protezione dei dati (DPIA) costituisce un adempimento derivante dal principio introdotto della responsabilizzazione (*accountability*) dei titolari nei confronti dei trattamenti da questi effettuati. La DPIA è richiesta obbligatoriamente in alcuni casi (valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su un trattamento automatizzato; trattamento, su larga scala, di categorie particolari di dati personali o dei dati relativi a condanne penali e a reati; sorveglianza sistematica su larga scala di una zona accessibile al pubblico).	*Artt. 35, 36 GDPR*
Formazione personale che tratta i dati personali	Il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso	*Artt. 29, 32, par. 4 e 39, par. 1, lett. c), GDPR*

Aspetti formali di adeguamento alla normativa *privacy*

Vs.

Aspetti sostanziali di adeguamento alla normativa *privacy*

- *Individuazione effettiva dei ruoli, dei compiti e delle responsabilità, con chiara definizione del sistema di deleghe (Modello organizzativo);*
- *Sistemi di controllo interno;*
- *Procedure relative al trattamento dei dati personali (raccolta, elaborazione, conservazione);*
- *Misure di sicurezza fisiche ed informatiche;*
- *Formazione.*

Accountability
Privacy by design
Privacy by default

2. NORMATIVA *PRIVACY* E ANTIRICICLAGGIO

La normativa relativa al trattamento dei dati personali (c.d. *privacy*) trova una **propria applicazione diretta ed immediata anche agli effetti della normativa antiriciclaggio.**

Nell'ambito della normativa antiriciclaggio (d.lgs. 21 novembre 2007, n. 231), inoltre, la normativa sulla *privacy* **è richiamata numerose volte.**

Principali norme contenute della disciplina antiriciclaggio che richiamano la normativa sulla *privacy*	
Norma	**Breve descrizione**
Art. 16, commi 3 e 4, d.lgs. n. 231 del 2007 **Procedure adottate ai fini del mitigazione del rischio di antiriciclaggio**	I soggetti obbligati adottano **misure proporzionate ai propri rischi, alla propria natura e alle proprie dimensioni**, idonee a rendere note al proprio personale gli obblighi cui sono tenuti ai sensi della normativa antiriciclaggio, **ivi compresi quelli in materia di protezione dei dati personali**. A tal fine, i soggetti obbligati devono garantire **lo svolgimento di programmi permanenti di formazione** finalizzati alla corretta applicazione delle disposizioni della normativa antiriciclaggio e delle relative procedure. I **sistemi e le procedure di mitigazione del rischio antiriciclaggio** devono rispettare le prescrizioni e garanzie stabilite dal presente decreto e dalla **normativa vigente in materia di protezione dei dati personali.**
Art. 32 d.lgs. n. 231 del 2007 **Modalità di conservazione dei dati e delle informazioni**	I soggetti obbligati devono adottare **sistemi di conservazione dei documenti, dei dati e delle informazioni idonei a garantire il rispetto delle norme dettate dal codice in materia di protezione dei dati personali, nonché il trattamento dei medesimi esclusivamente per le finalità di cui al decreto 231 del 2007.**

Principali norme contenute della disciplina antiriciclaggio che richiamano la normativa sulla *privacy*

Norma	Breve descrizione
Art. 38 d.lgs. n. 231 del 2007 **Tutela del segnalante della SOS**	I soggetti obbligati devono adottare **tutte le misure idonee ad assicurare la riservatezza dell'identità delle persone che effettuano la segnalazione**. La **trasmissione delle SOS, le eventuali richieste di approfondimenti, nonché gli scambi di informazioni, attinenti alle OS segnalate avvengono per via telematica, con modalità idonee a garantire la tutela della riservatezza**, la riferibilità della trasmissione dei dati ai soli **soggetti interessati**, nonché **l'integrità delle informazioni trasmesse.**
Art. 39 d.lgs. n. 231 del 2007 **Divieto di comunicazione delle SOS**	Fuori dai casi previsti dal decreto, **è fatto divieto ai soggetti tenuti alla SOS e a chiunque ne sia comunque a conoscenza, di dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione,** dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza ovvero della probabilità di indagini o approfondimenti in materia di riciclaggio o di finanziamento del terrorismo. **Nei casi relativi allo stesso cliente o alla stessa operazione, che coinvolgano due o più professionisti**, il divieto non impedisce la comunicazione tra i professionisti in questione, a condizione che appartengano ad uno Stato membro UE o siano situati in un Paese terzo che impone obblighi equivalenti a quelli previsti dalla normativa antiriciclaggio e dal GDPR in materia di trasferimento di dati a Paesi Terzi. **Le informazioni scambiate possono essere utilizzate esclusivamente ai fini di prevenzione del riciclaggio o del finanziamento del terrorismo.**

Pertanto, la corretta effettuazione delle procedure e degli obblighi previsti dalla normativa antiriciclaggio **dovrà attentamente considerare** i **principi della normativa sulla *privacy*.**

Il Professionista è, al contempo:

- **Soggetto obbligato ai fini della normativa antiriciclaggio** *(art. 3, comma 4, d.lgs. n. 231 del 2007);*
- **Titolare del trattamento dei dati personali ai fini della normativa sulla *privacy*** *(art. 4, par. 1, n. 7, GDPR).*

Occorrerà, dunque, considerare le **relazioni tra normativa antiriciclaggio e *privacy***.

Soggetti. Nell'ambito della normativa antiriciclaggio, ordinariamente:

a) Il **professionista** assume ordinariamente il ruolo di **titolare del trattamento dei dati del cliente/interessato.**
b) I **soggetti interni** all'organizzazione, riconducibili alla Funzione antiriciclaggio, che collaborano con il professionista (es. collaboratori della funzione antiriciclaggio) sono soggetti **«designati» o «autorizzati»** al trattamento dei dati personali.
c) I **collaboratori esterni** sono «**contitolari del trattamento**» (es. altri professionisti che seguono la medesima pratica/cliente *ex* art. 39, comma 5, d.lgs. n. 231 del 2007) o «**responsabili del trattamento**» (es. conservazione presso terzi *ex* art. 32, comma 3, d.lgs. n. 231 del 2007; adeguata verifica da parte di terzi *ex* artt. 26-30, d.lgs. n. 231 del 2007).

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Principi. I principi previsti dal GDPR si **applicano anche nell'ambito della normativa antiriciclaggio.** La normativa antiriciclaggio comporta, infatti, per il professionista/titolare del trattamento/soggetto obbligato il **trattamento di dati personali** del cliente/interessato.

La **base giuridica** del trattamento dei dati personali necessari per adempiere agli obblighi antiriciclaggio discende da un **obbligo legale** al quale il Professionista/Titolare del trattamento è soggetto, ovverosia dalla **normativa antiriciclaggio stessa** (d.lgs. n. 231 del 2007). Ciò significa che **non occorre il consenso** dell'interessato/cliente affinché il professionista adempia agli obblighi antiriciclaggio. ► ***Principio di liceità del trattamento.***

Il cliente dovrà essere informato, **mediante la somministrazione di apposita informativa (art. 13 GDPR),** che i dati del cliente/interessato **saranno trattati anche ai fini della normativa antiriciclaggio** ► ***Principio di trasparenza.***

I dati richiesti al cliente/interessato a detti fini dovranno essere solo quelli **necessari** ad adempiere alla normativa antiriciclaggio ► ***Principio di minimizzazione dei dati.***

(continua nella slide successiva)

(continua dalla slide precedente)

I dati raccolti ai fini antiriciclaggio potranno essere trattati **solo a tali fini** ► ***Principio di limitazione della finalità.***

I dati raccolti dovranno essere trattati approntando le **misure organizzative e tecniche necessarie a garantire la sicurezza dei dati e la conformità del trattamento, che dovranno essere approntate prima che il trattamento abbia inizio** ► ***Principi di "accountability, "privacy by design" e "privacy by default" e del rischio inerente al trattamento (risk based approach)***

I dati raccolti ai fini antiriciclaggio dovranno essere conservati al massimo **per 10 anni.**
► ***Principio di limitazione della conservazione.***

Non potrà essere esercitato da parte del cliente/interessato il diritto alla cancellazione dei dati (diritto all'oblio) poiché in tal caso cui la richiesta di cancellazione dei dati contrasta con l'adempimento di un obbligo giuridico di fonte legislativa cui è soggetto il titolare del trattamento ► ***Principio di bilanciamento degli interessi.***

Come anticipato, nell'ambito della normativa antiriciclaggio (d.lgs. 21 novembre 2007, n. 231) la normativa relativa al trattamento dei dati personali (c.d. *privacy*) **è richiamata numerose volte.**

Il Legislatore ha, dunque, voluto dedicare una **particolare attenzione** al trattamento dei dati personali acquisiti nell'ambito degli obblighi previsti dalla normativa antiriciclaggio.

In definitiva, le importanti relazioni esistenti tra normativa sulla *privacy* e antiriciclaggio dovrebbero condurre il professionista o lo studio professionale a progettare ed attuare un «**unico modello organizzativo integrato *privacy*-antiriciclaggio**».

Compliance integrata
Antiriciclaggio - Privacy

Operativamente occorrerà progettare ed attuare un sistema di ***compliance* integrato** in merito:

- Alla **gestione del mandato professionale;**

- Alla **gestione dei sistemi e alle procedure organizzative**:

- *Adozione di sistemi di controllo interno e procedure di valutazione del rischio;*
- *Procedure e agli obblighi relativi all'adeguata verifica della clientela;*
- *Procedure e obblighi di conservazione;*
- *Procedure e obblighi di segnalazione delle operazioni sospette (SOS);*
- *Procedura relativa alla formazione.*

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Gestione integrata del mandato professionale.

A. Somministrazione lettera di incarico professionale;
B. Somministrazione informativa *privacy* (con specifica indicazione degli obblighi antiriciclaggio);
C. Somministrazione modulo di identificazione e di adeguata verifica della clientela.

Gestione dei sistemi e alle procedure organizzative:

A. Adozione di sistemi di controllo interno e procedure di valutazione del rischio;
B. Procedure e agli obblighi relativi all'adeguata verifica della clientela;
C. Procedure e obblighi di conservazione;
D. Procedure e obblighi di segnalazione delle operazioni sospette (SOS);
E. Procedura relativa alla formazione.

A) Gestione integrata dei sistemi e delle procedure organizzative:

Sistemi di controllo interno e procedure di valutazione del rischio:

- Adozione di presidi e attuazione di controlli interni e procedure organizzative, adeguati alla propria natura e dimensione, necessari a mitigare e gestire i rischi di riciclaggio e di finanziamento del terrorismo;
- Adozione di misure tecniche ed organizzative adeguate alle singole realtà operative, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento dei dati personali, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche *(rischio inerente al trattamento)*;

Principio del *Risk based approach* ai fini antiriciclaggio e ai fini della normativa *privacy.*

- Verifica delle lettere di incarico autorizzati/responsabili del trattamento - Funzione Antiriciclaggio.

(Continua slide successiva)

B) Procedure e obblighi relativi all'adeguata verifica della clientela

- Somministrazione informativa sulla *privacy*;
- Pertinenza e finalità del dato raccolto/trattato.

(Continua slide successiva)

C) Procedure e obblighi di conservazione

- Gestione integrata del fascicolo della clientela (lettera di incarico professionale; informativa *privacy;* modulo di identificazione e di adeguata verifica della clientela; documenti identità; valutazione del rischio; documenti di approfondimento sulla posizione del cliente; documenti inerenti alla prestazione svolta; altro:es. *Memo* di aggiornamento periodico).
- Verifica del rispetto del criterio civilistico di 10 anni relativo al periodo di conservazione dei documenti rilevanti ai fini contabili, tributari e antiriciclaggio (cfr. Documento FNC-CNDCEC dell'Aprile 2018);
- Integrità del dato;
- Sistemi di sicurezza fisici ed informatici.

(Continua slide successiva)

D) Procedure e obblighi di segnalazione delle operazioni sospette (SOS)

- Tutela identità segnalante;
- Tutela segnalazione (SOS);
- Integrità del dato.

- ***Deroga al segreto professionale ex art. 35, comma 4, d.lgs. n. 231 del 2007****: Le comunicazioni delle informazioni, effettuate in buona fede dai soggetti obbligati, dai loro dipendenti o amministratori ai fini della segnalazione di operazioni sospette,* ***non costituiscono violazione*** *di eventuali restrizioni alla comunicazione di informazioni imposte in sede contrattuale o da disposizioni legislative, regolamentari o amministrative.* ***Nella deroga deve ritenersi ricompresa anche la normativa sulla privacy.***

- ***«Deroga della deroga» ex art. 35, comma 5, d.lgs. n. 231 del 2007: L'obbligo di SOS non si applica*** per le informazioni che i professionisti ricevono da un loro cliente o ottengono riguardo allo stesso nel corso dell'esame della posizione giuridica o dell'espletamento dei compiti di difesa o di rappresentanza del medesimo in un procedimento innanzi a un'autorità giudiziaria o in relazione a tale procedimento, compresa la consulenza sull'eventualità di intentarlo o evitarlo, ove tali informazioni siano ricevute o ottenute prima, durante o dopo il procedimento stesso.

(Continua slide successiva)

E) Procedura relativa alla formazione

- Formazione permanente e continua in materia di antiriciclaggio e *privacy* (anche congiunta, vd. art. 16, d.lgs. n. 231 del 2007).

a) **SANZIONI NORMATIVA *PRIVACY* PER IL TITOLARE DEL TRATTAMENTO.**

b) **Sanzioni amministrative** *(artt. 83-84 GDPR).* **Pene pecuniarie variabili fino a 20 ml €,** o per le imprese, fino al **4% del fatturato mondiale** totale annuo dell'esercizio precedente;

c) **Sanzioni penali** (*art. 167 e ss, d.lgs. n. 196 del 2003, come da ultimo modificato dal d.lgs. n. 101 del 2018*). Per alcuni reati è prevista la **reclusione fino a 3 anni.**

Es. Reclusione da 6 mesi a tre anni per falsità nelle dichiarazioni al Garante.

SANZIONI NORMATIVA ANTIRICICLAGGIO PER I SOGGETTI OBBLIGATI.

i. **Sanzioni amministrative** *(art. 55 e ss, d.lgs. n. 231 del 2007, da ultimo modificato dal d.lgs. n. 90 del 2017).* **Pene pecuniarie variabili.**

Es. Sanzione da 2.000 € fino a 50.000 € nel caso di inosservanza degli obblighi di adeguata verifica, di conservazione e di astensione dallo svolgimento dell'incarico; Sanzione da 3.000 a 1 mln € nel caso di violazioni concernenti la SOS; Sanzione da 3.000 € a 15.000 € per non aver segnalato operazioni in denaro contante oltre soglia.

i. **Sanzioni penali** (*art. 55 e ss, d.lgs. n. 231 del 2007, da ultimo modificato dal d.lgs. n. 90 del 2017*). Per alcune fattispecie, oltre alla multa, è prevista la **reclusione**.

Es. Multa da 10.000 € a 30.000 € e reclusione da 6 mesi a 3 anni nel caso di falsificazione dei dati relativi all'adeguata verifica della clientela oppure utilizzo cosciente di dati falsi ai medesimi fini; Multa da 5.000 € a 30.000 € e reclusione da 6 mesi ad 1 anno nel caso di divulgazione, colposa o dolosa, dell'avvenuta SOS, (salvo le eccezioni, es. comunicazioni tra professionisti di uno stesso Studio o che lavorano su una medesima pratica).

«Cumulabilità» tra sanzioni normativa *privacy* e antiriciclaggio «procedurale» e «sostanziale»?

Importanza di
<u>Compliance integrata</u>
Antiriciclaggio - Privacy