e-book

A cura di Giuseppe Miceli
Autori: Giuseppe Miceli, Marco Miceli, Luca Malatesta

LA PRIVACY NEGLI STUDI PROFESSIONALI

Schemi riepilogativi e consigli pratici per gli adempimenti

Focus operativo su ispezioni e sanzioni

ESTRATTO OMAGGIO

FISCO e TASSE .com
la tua guida per un fisco semplice

MAGGIOLI EDITORE

A cura di Giuseppe Miceli

Autori: Giuseppe Miceli, Marco Miceli, Luca Malatesta

LA PRIVACY NEGLI STUDI PROFESSIONALI

Schemi riepilogativi e consigli pratici per gli adempimenti

Focus operativo su ispezioni e sanzioni

Formulario

FISCO e TASSE .com
la tua guida per un fisco semplice
MAGGIOLI EDITORE

Giuseppe Miceli

Legal Advisor - Giurista abilitato alla professione forense.
Laureato presso l'Università degli studi di Roma *"La Sapienza"* con tesi di laurea in diritto processuale penale, dal titolo *"Prove penali e inutilizzabilità"*. Abilitazione alla professione di Avvocato nel 2008, presso la Corte d'Appello di Roma. Docente al Master "*Manager dei processi innovativi nelle start-up culturali e creative*" presso l'Università degli Studi Camerino*;* ai Master in *"Data Analyst"* e in *"Sicurezza delle reti informatiche"* dell'Università Niccolò Cusano. Relatore in numerosi convegni accreditati presso *l'Ordine degli Avvocati di Roma e Ancona e Ordine dei Consulenti del Lavoro di Roma.* Componente esterno, Esperto in materia di Antiriciclaggio, del Centro Studi dell'Ordine dei Consulenti del Lavoro di Roma.

Marco Miceli

Pluriennale esperienza nel mondo HR. Ha rivestito sin da giovane responsabilità presso multinazionali, gestendo importanti progetti e obiettivi.
Esperto conoscitore di tutte le tematiche HR come *recruiting*, selezione *&* formazione, riorganizzazioni e *star up* aziendali, *compensation*, gestione degli ambienti di lavoro, gestione della corretta applicazione delle normative legislative e contrattuali per il personale in materia di lavoro, fiscale, previdenziale e assistenziale, *welfare*, sviluppo e *change management*, *budgeting*, contrattazione aziendale e relazioni sindacali.
Attualmente *Reporting & Reporting Manager*, presso la Direzione Risorse Umane di un importante Gruppo che opera nell'ambito delle tecnologie avanzate ambito trasporti, coordina un *team* di risorse per importanti progetti internazionali.

Luca Malatesta

Avvocato con più di 15 anni di esperienza nella consulenza direzionale, forte del *background* nel campo delle telecomunicazioni e dell'informatica, si interessa della *compliance* delle grandi aziende internazionali e delle PMI italiane. Nel 2005 a lavorare alla figura del Global@ccount®, ovvero il consulente multidisciplinare. Più tardi crea *Insight*, piattaforma *software* proprietaria per la gestione di *audit* e *compliance* normativa e attorno alla piattaforma crea MBS - *My Business Solutions*, un coagulo di competenze ed eccellenze professionali, di cui è Amministratore e coordinatore delle direzioni scientifiche incaricate di trasformare il proprio know-how in valore aggiunto sulla piattaforma.

ISBN: 9788868058449

Settembre 2019

www.fiscoetasse.com

FISCO eTASSE .com
la tua guida per un fisco semplice

Indice

Prefazione

Il 27 Aprile 2016 la Commissione Europea ha presentato il Regolamento 679/2016 per l'aggiornamento della normativa concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati. Il Regolamento UE, essendo un atto *self executive*, ai sensi dell'art. 288 del Trattato sul funzionamento della Comunità Europea, è direttamente esecutivo e non necessita di recepimento da parte degli stati membri, cosicchè a decorrere dal 25 Maggio 2018, la normativa succitata è diventata immediatamente applicabile anche nello Stato italiano. L'intero Regolamento 679/2016 è costellato da una costante dialettica tra tecnica e libertà, innovazione e diritti, iniziativa economica e garanzie. Significativa è l'esigenza di adeguamento della disciplina alla realtà nella sua evoluzione tecnologica. Non vi è dubbio, infatti, che tanto le norme giuridiche quanto le norme tecniche formano ormai un sistema fortemente interconnesso rispetto a qualunque uso corretto dei dati , in particolare con riguardo alla legittimità della raccolta, uso e conservazione di quelli personali ed è altrettanto vero che redigere una collettanea che descriva il rapporto tra nuove tecnologie e mondo giuridico è una sfida che si presenta impossibile da vincere per il rischio che le nozioni espresse diventino obsolete al momento della pubblicazione . Bene hanno fatto gli autori a proporre una pubblicazione snella, che trattasse ed avvicinasse i cittadini, siano essi professionisti o imprenditori, al mondo della protezione dei dati. Ciò che trasuda da questa collettanea è un grande senso di legalità e di conoscenza delle norme espresse in modo semplice e costruttivo e voglio augurarmi che in un futuro, spero prossimo, decidano di cimentarsi con altre sfide letterarie , li leggeremo sempre con piacere.

Giulio Botta

Presidente Associazione Europea Protezione Dati

Via Flaminia 392

60126 Ancona

Premessa

(Avv. Luca Malatesta)

A poco più di un anno dal 25 maggio 2018, termine ultimo per l'applicazione del Regolamento Generale Europeo Per La Protezione Dei Dati, che tutti ormai conosciamo attraverso l'acronimo inglese GDPR, la politica dei grandi numeri, delle grandi aziende e dei grandi gruppi lo sbandiera come un grande successo politico soprattutto in Europa. Il Regolamento, infatti, nella realtà delle imprese medio-grandi, globalizzate e mondiali è diventato lo standard di riferimento adottato tout-court "*dai paesi che costituiscono il 42% del PIL mondiale e il 34% degli scambi globali*[1]" con l'effetto molto pratico che chiunque abbia attività transnazionali di qualche tipo con un paese occidentale debba in qualche modo farci i conti.

La parte di più faticosa applicazione per un professionista regolamentato che operi sul mercato italiano e che debba lavorare per la conformità normativa del proprio studio professionale ovvero dell'attività di un cliente, secondo la personale esperienza di chi scrive, sta proprio nella struttura stessa della normativa.

Il legislatore europeo, infatti, nella redazione del Regolamento ha attinto a piene mani dai **paradigmi aziendali di "automiglioramento" e "autovalutazione" propri delle cosiddette normative volontarie**, come gli standard internazionali di qualità che pongono in capo al titolare del trattamento prima ancora che un obbligo di adeguamento a dei parametri normativamente previsti, il non facile compito di stabilire quali misure siano nel pratico sufficienti ed adeguate alla tutela dei dati che gli vengono affidati dall'interessato. Ne discende, sotto l'ombrello della responsabilizzazione del titolare, quel principio di *accountability* ormai entrato nel lessico comune degli operatori che abbiano a che fare con la riservatezza, una **grande difficoltà per l'operatore pratico**, tradizionalmente abituato a ritenere la *compliance* come una serie di esatti adempimenti che scaturivano dal dettato normativo del vecchio codice.

A questo deve aggiungersi anche il fatto che la lunga gestazione del GDPR ha fatto sì che le autorità politiche e di governo europee, in particolare alcune fossero soggette ad enormi pressioni di lobbying come denunciato dal Garante della Privacy Antonello Soro nella *lectio magistralis* tenuta all'Università di Firenze il 4 marzo 2019. Ne è uscita fuori una legislazione che, a parere di chi scrive, risulta

[1] Martin Selmayr, Segretario generale della Commissione Juncker, 16 mag 2019.

eccessivamente tagliata per le grandi aziende multinazionali, basti pensare all'istituto dell'*one-stop-shop* che permette ai colossi dell'informatica di scegliersi in pratica con quale garante nazionale avere un'interlocuzione privilegiata, mentre delega alle autorità garanti nazionali un'impressionante opera di *soft law* per promulgare regolamenti di dettaglio applicabili a singole categorie o fattispecie. Nell'attesa che le autorità garanti smaltiscano questo enorme carico di lavoro, il GDPR con tutto il suo apparato sanzionatorio è pienamente in vigore anche per i professionisti che dovranno **tradurre nella realtà** dei loro studi la normativa, in azioni concrete, anche senza necessariamente far ricorso a uffici *compliance* come quelli delle grandi aziende, ovvero costosi consulenti esterni.

Un approccio che può certamente aiutare nella pratica, nonostante la stragrande maggioranza dei contributi reperibili ponga il titolare del trattamento al centro di normative, azioni, contromisure, è porre l'accento, invece, sull'interessato.

Un titolare del trattamento, nel nostro caso il **professionista**, è infatti il **primo garante della regolarità del trattamento.** L'aderenza al GDPR comporta infatti la comprensione di tutta la serie di regole di condotta che il titolare deve all'interessato in cambio del conferimento dei suoi dati, a cominciare dalla preventiva predisposizione del materiale da sottoporre allo stesso, non tanto al fine di farsi sottoscrivere un foglio di carta per un'eventuale esclusione di responsabilità, ma perché la consapevolezza che si sta lavorando basandosi su una proprietà altrui che viene conferita al professionista, sia esso titolare o responsabile del trattamento, per l'espletamento di un mandato, e che quindi **l'interessato avrà il pieno diritto di conoscere e controllare tipologia, esiti e finalità del trattamento.**

Focus - Attività di ispezione e impianto sanzionatorio

(Dott. Giuseppe Miceli)

a) Le ispezioni: operatività e consigli utili

Con la *newsletter* del 25 marzo 2019 Il Garante per la Privacy ha pubblicato - sul sito *www.garanteprivacy.it* - la Deliberazione del 14 febbraio 2019 relativa all'attività ispettiva effettuate dall´Ufficio nel primo semestre 2019, anche in collaborazione con il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, del Corpo della Guardia di Finanza[77].

Tale attività ispettiva è prevista e disciplinata al Capo III - *Accertamenti e controlli* - del Codice privacy, in particolare gli artt. 157 (*richiesta di informazioni e documenti*) e 158 (accertamenti) del codice privacy.

Deve tenersi conto che le attività ispettive e di controllo in materia di privacy, così come previste e disciplinate dal GDPR hanno abbandonato l'obsoleto carattere di "staticità" tipizzato in una mera spunta della c.d. *"check-list privacy"* e hanno assunto il carattere della "dinamicità" che contraddistingue la ricerca continua e pro-attiva di *compliance* rispetto al GDPR, alla normativa nazionale e ai provvedimenti delle Autorità di controllo.

In pratica: in fase di attività ispettiva potrà anche emergere la mancata adozione di una "misura" di protezione dei dati personali (per esempio, la nomina del DPO) tuttavia, non automaticamente ne scaturirà la contestazione e la sanzione.

Determinante sarà – sulla base del principio di *accountability* – la condotta del titolare del trattamento, sottoposto al controllo, che potrà dare dimostrazione (Comprovare) sulla base della ricostruzione logico-giuridica che non si tratti di un mancato adempimento, bensì del legittimo risultato di una attenta valutazione.

Dirimente, pertanto, in fase di ispezione, è la capacità del titolari o responsabile del trattamento di saper dare conto – in maniera *accountability* - delle scelte operate e delle decisioni applicate.

[77] Tale collaborazione è frutto del Protocollo d'Intesa tra Garante della Privacy e Guardia di Finanza, siglato il 10 marzo 2016 che tratta: della gestione dei rapporti con l'Autorità Garante; dell'esecuzione di ispezioni su delega dell'Autorità Garante; partecipazione a ispezioni congiunte con l'Autorità; dello sviluppo di attività progettuali in sinergia con i Reparti territoriali del Corpo della G. di F. e, infine, dell'individuazione soggetti da proporre quali destinatari delle ispezioni. In relazione a quest'ultimo aspetto, si rileva che le ispezioni vengono svolte non esclusivamente nei confronti dei soggetti nei confronti dei quali gli interessati abbiano trasmesso reclami o segnalazioni.

I poteri ispettivi del Garante consentono l'accesso a banche dati, archivi nei luoghi in cui si svolge il trattamento o nei quali è necessario effettuare verifiche utili al controllo del rispetto della normativa sul trattamento dei dati personali. Inoltre, il Garante può chiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile nominati, all'interessato o anche a terzi di fornire informazioni o di esibire documenti anche in relazione a banche dati.

Ai sensi dell'art. 158, c.4, del Codice privacy, se l'ispezione disposta dal Garante deve svolgersi in una abitazione o un altro luogo di dimora privata è necessario *"l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento"*[78].

L'accertamento non può essere iniziato prime delle ore sette e dopo le ore venti salvo diversa disposizione del decreto del presidente del Tribunale.
In caso di rifiuto gli accertamenti sono comunque eseguiti e le spese ove occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento.

È bene evidenziare che le ispezioni possono avvenire a sorpresa oppure, in alcuni casi, a seguito di avviso del Garante o della Guardia di Finanza che ne possono dare comunicazione tramite posta elettronica, il giorno prima del sopralluogo.
Attenzione: in alcuni casi l'impresa o lo studio professionale, in quanto titolari o responsabili del trattamento, possono ricevere la sola richieste di informazioni da parte dell'Autorità, senza l'espressa previsione di una successiva attività di ispezione. Ebbene, in tali casi il livello di esaustività delle informazioni fornite dal Titolare/Responsabile del trattamento sarà inversamente proporzionale alla probabilità che si realizzi una conseguente attività ispettiva da parte del Garante. Ciò significa che si dovrà prestare massima attenzione e solerzia nel soddisfare la richiesta di informazioni, affinchè possa dissiparsi la necessità del Garante di procedere all'ispezione.

[78] In quest'ultimo caso dovrà essere rilasciata una copia del provvedimento di autorizzazione del Tribunale alla parte.

Sul piano operativo è bene evidenziare che contestualmente alle operazioni di accesso, **gli ispettori esibiscono – oltre alle tessere di riconoscimento[79] - la "*richiesta di informazioni*"** ovvero documento con il quale il Garante chiede al soggetto sottoposto a ispezione di dare conto degli obblighi – auspicabilmente – assolti, in materia di protezione dei dati personali, nonchè delle modalità di adempimento[80]. Lo stesso documento, dunque, è di fondamentale importanza, dato che individua il "perimetro" delle attività ispezione cui si inizia a dare corso.

Con il documento di richiesta di informazioni il Garante può chiedere di dare conto, per esempio: delle modalità attraverso cui gli interessati vengono portati a conoscenza dell'informativa; di come viene raccolto il consenso (se necessario); delle nomine di eventuali responsabili del trattamento (interni o esterni); delle modalità di conservazione dei dati personali e dei criteri di definizione della durata dei trattamenti stessi; delle misure di sicurezza di cui si sia dotato il titolare o responsabile del trattamento sottoposto all'attività ispettiva e in ultimo – ma non per importanza – può essere richiesto al titolare di "comprovare" di aver provveduto alla formazione obbligatoria (almeno a scadenze annuali e comunque in stretta relazione al trattamento dei dati svolto in azienda) dei dipendenti. Esibendo idonea documentazione a supporto.

N.B.: l'art. 83.4 GDPR fissa per la mancata erogazione della formazione la sanzione fino a 10 milioni di euro o, per le imprese, fino al 2 % del fatturato mondiale annuo dell'anno precedente se superiore.

Ecco quindi che proprio il momento in cui si innesca l'attività ispettiva può assumere importanza determinante rispetto all'esito della verifica.

Se è vero, come è vero, che la "*richiesta di informazioni*" è utile alla parte assoggettata al controllo, in quanto è sulla base di tale documento che si dovranno delimitare i poteri di controllo del Garante, è altrettanto vero che l'inadempimento alla richiesta di informazioni e la mancata esibizione dei documenti in essa indicati potrà comportare l'irrogazione di una sanzione pecuniaria fino a venti milioni di euro o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

[79] Si ricorda che le attività ispettive sono condotte in genere dai militari del Nucleo Speciale Privacy della Guardia di Finanza che possono essere, o meno, accompagnati dai funzionari del Garante. Specularmente, in altri casi, sono i funzionari del Garante a procedere alle ispezioni con o senza il supporto dei finanzieri.

[80] L'obbligo formativo è previsto dall'art. 39.1.b del GDPR, che indica tra i compiti del DPO quello di: "*sorvegliare l'osservanza* […] *delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi* […] *la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*"; inoltre l'art. 29 e l'art. 32.4 sanciscono che *"chiunque abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento".*

Attenzione: Il consiglio più opportuno è, dunque, quello di prestare massima attenzione alla fase di presentazione degli ispettori e a quella di approccio all'attività ispettiva e di non lesinare i dovuti atti di collaborazione pro-attiva.

Restando sul piano dell'operatività, al titolare o responsabile del trattamento nei cui confronti si sta svolgendo l'ispezione, potrà risultare particolarmente utile chiedere di esercitare la facoltà di farsi assistere, già dalle prima fasi della verifica, da consulenti di fiducia (avvocato esperto in materia di privacy o consulente tecnico informatico). Mentre, invece, diamo per scontata la presenza del DPO (ove sia stato nominato) se non altro perché - come è noto – tra i suoi principali doveri vi è quello di fungere da interfaccia con l'Autorità di controllo.

Altrettanto delicata e importante è la fase in cui gli ispettori procedono – nel contraddittorio con la parte - alla **redazione del verbale di operazioni** compiute.

Si tratta della fase in cui vengono verbalizzate tutte le attività svolte e le modalità di svolgimento, a partire dall'accesso e fino alla chiusura dell'attività ispettiva o alla sua sospensione, nel caso in cui le attività dovessero interrompersi per poi riprendere il giorno seguente o dopo una interruzione dettata da altri motivi.

Il verbale - redatto a cura degli ispettori – potrà riportare eventuali dichiarazioni della parte o dei presenti alle attività di verifica (premesso che ciascun presente dovrà essere formalmente identificato tramite documenti di identità).

La corretta applicazione di un presidio privacy *compliant* potrà emergere dalla istituzione di un *team privacy* composto da: DPO, esperto informatico (responsabile ICT) capo responsabile aziendale della funzione *compliance* e responsabile del trattamento (che in molti casi corrisponde al Direttore HR). Il *team privacy* dovrà essere reperibile e operativo già nella fase di avvio di ispezione, ciò per evitare o, almeno, limitare i rischi di incorrere in contestazioni sanzionatorie.

Attenzione:

È consigliabile che il Titolare del trattamento individui la figura appartenete al *team privacy* cui affidare l'incarico preciso di fungere da interfaccia con le Autorità di controllo.

È auspicabile che tale incarico sia assegnato al DPO (ove nominato).

Oltretutto, la previsione di un "protocollo di attivazione" del *team privacy* aziendale è, di per sé, segnale di *compliance*. Gli ispettori, infatti, potranno constatare l'adozione di un protocollo di attivazione che,

evidentemente si applicherà anche in caso di *data breach*.

Attenzione:

Il consiglio è quello di chiedere di poter leggere e di verificare la correttezza delle dichiarazioni rilasciate e verbalizzate. Tanto più che la dicitura presente in calce al verbale *"letto e sottoscritto"* (anche dalla parte e dai presenti) lascerebbe scarso adito a ipotesi di incongruenza tra quanto dichiarato (dalla parte) e quanto scritto – *rectius*, verbalizzato – (dal Pubblico Ufficiale).

In ogni caso, è bene sapere che la parte ha a disposizione – in linea generale - **quindici giorni (a partire dalla data di apertura delle operazioni di ispezione) per produrre la documentazione** eventualmente richiesta dagli ispettori.

Attenzione:

Si consiglia di tenere in massima considerazione il rispetto di tale scadenza che – oltretutto – denota la corretta attuazione del principio di *accountability,* la incapacità – dichiarata, più o meno esplicitamente – di reperire i documenti richiesti sarebbe un evidente segnale di "non *compliant".*

Inoltre, si consiglia di consegnare solo copia della documentazione richiesta, in quanto l'originale dovrà essere – eventualmente – esibito in sede di ispezione.

b) Provvedimenti del Garante: sanzioni e provvedimenti correttivi

La **fase post-ispettiva** è quella in cui l'Autorità Garante per la protezione dei dati personali esercita il potere di comminare le sanzioni amministrative pecuniarie o di emanare i provvedimenti correttivi.

Rispetto all'applicazione delle **sanzioni pecuniarie**, l'art. 166 del Codice privacy ne attribuisce la **competenza al Garante per la privacy** che potrà, quindi, irrogare le sanzioni pecuniarie previste dall'art. 83 del GDPR e i provvedimenti correttivi di cui all'art. 58 paragrafo 2 del GDPR.
Lo stesso menzionato art. 166 Codice privacy sancisce che sono soggette alla sanzione amministrativa dell'art. 83 paragrafo 4 del GDPR, ovvero fino a 10 milioni di euro o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, le violazioni di cui agli articoli 2-*quinquies*, comma 2, 2-*quinquiesdecies*, 92, comma 1, 93, comma 1, 123, comma 4, 128, 129, comma 2, e 132-*ter*, nonché la mancata effettuazione della DPIA nei casi previsti dall'art. 110 comma primo.
Il paragrafo 5 dell'art. 83 GDPR prevede le sanzioni di maggiore entità, ovvero fino a 20 milioni di euro o per le imprese fino al 4% del fatturato, applicabili alle violazioni più gravi.

In fase di applicazione delle sanzioni pecuniarie, il Garante dovrà considerare, oltre alle circostanze del caso in esame, anche le caratteristiche del soggetto trasgressore e la collaborazione eventualmente

prestata, ancora, l'entità del danno arrecato agli interessati e il numero degli interessati esposti ai rischi della violazione.
in tal modo, il Garante potrà valutare l'ammontare della sanzione da comminare garantendo, così, che la sanzione sia *effettiva, proporzionata e dissuasiva,* così come previsto dal legislatore comunitario nel testo del Regolamento generale.

Attenzione: vi sono fattispecie suscettibili di poter essere verificate "da remoto" da parte dell'Autorità di controllo.

Si pensi, ad esempio, alla violazione di quanto previsto dal comma 7 dell'art. 37 del GDPR che pone l'obbligo per il titolare o responsabile del trattamento di rendere pubblici i dati di contatto del proprio *Data Protection Officer* (DPO) e di comunicarli all'Autorità Garante per la Protezione dei Dati Personali (la fattispecie si applica nei casi in cui la nomina del DPO sia obblifigatoria).

Tale violazione prevede una sanzione amministrativa fino a € 10.000.000 o al 2% del fatturato mondiale (ove superiore) per il trasgressore.

Per non incorrere in tale violazione:

2) i dati di contatto del DPO, possono essere resi pubblici mediante pubblicazione sul sito *web* istituzionale di un'apposita pagina dedicata all'esercizio dei diritti dell'interessato o tramite il loro inserimento nell'informativa privacy e la pubblicazione di quest'ultima *on-line*;
3) la comunicazione del nominativo del *Data Protection Officer* al Garante Privacy, deve essere effettuata mediante una procedura di invio telematico. Il Garante per la Privacy ha istituito un sistema di Comunicazione dei dati di contatto del Responsabile della Protezione dei Dati – RPD o DPO.

In virtù degli artt. 58.2 GDPR e 166.3 del Codice privacy, Garante può adottare una serie di provvedimenti correttivi. Si tratta del **potere di rivolgere avvertimenti al titolare o al responsabile** del trattamento sulla base di quei trattamenti considerati a rischio di violazione delle disposizioni del GDPR. In questi casi, il Garante può rivolgere ammonimenti o ingiungere di dare riscontro alle richieste avanzate dall'interessato, inn ordine – per esempio – all'esercizio dei diritti previsti dal GDPR.

Nel caso in cui l'Autorità di controllo dovesse ritenere configurati gli elementi da cui emergerebbe la violazione (o le violazioni) previste dal Codice Privacy o dall'art. 83 GDPR, ai sensi dell'art. 166 del Codice, dovrà procedere alla notifica al titolare o al responsabile del trattamento delle presunte violazioni *"salvo che la previa notifica non sia compatibile con la natura del provvedimento che intende adottare"*.

Attenzione:

Il titolare o responsabile del trattamento al quale sia stata notificata la presunta violazione, entro trenta giorni dal ricevimento, potrà inviare al Garante scritti difensivi o documenti e chiedere di essere ascoltato.

Al termine della fase istruttoria, dopo aver esaminato le dichiarazioni difensive della parte, il Garante potrà decidere di comunicare il provvedimento sanzionatorio (ordinanza-ingiunzione). In tal caso, il trasgressore dispone di trenta giorni per potersi adeguare alle prescrizioni del Garante ed effettuare il pagamento di un importo pari alla metà della sanzione irrogata.

In alternativa, sempre nel termine perentorio di trenta giorni, il trasgressore ha facoltà di proporre ricorso innanzi all'Autorità Giudiziaria, presso il Tribunale del luogo ove il titolare del trattamento risiede oppure del luogo di residenza dell'interessato.

Attenzione: il Garante può applicare la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione sul sito internet (ai sensi dell'art. 166 comma 7). Si tratta di una circostanza che rischierebbe di intaccare la reputazione dell'impresa o dello studio professionale destinatario della sanzione.

Il novellato Codice della privacy, inoltre, prevede alcune **violazioni che assumono rilevanza penale.**

– Trattamento illecito di dati
– Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala
– Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala
– Interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante
– Inosservanza di provvedimenti del Garante
– Violazioni in materia di controlli a distanza dei lavoratori e di indagine sulle loro opinioni
– False attestazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante
– Inosservanza di provvedimenti del Garante