Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

Ordine degli Avvocati di Torino

Ordine degli Ingegneri della Provincia di Torino

Tavolo di lavoro congiunto "Protezione dei dati personali – GDPR"

Checklist di base per prepararsi al regolamento generale sulla protezione dei dati

riepilogo schematico per gli studi professionali

a cura del Referente del TdL congiunto «Protezione dei dati personali – GDPR»
Ordine degli Avvocati

Claudio STRATA *Avvocato*

Torino, 12 marzo 2018

GDPR – Responsabilità e deleghe – aspetti sanzionatori

RESPONSABILITA' E DELEGHE

Premessa di carattere generale

Principio di responsabilizzazione…… ***accountability***: si chiede al titolare del trattamento di porre in essere **misure tecniche e organizzative adeguate** per garantire che il trattamento sia effettuato conformemente al regolamento. **Non sono sufficienti le adesioni a codici di condotta o ad un meccanismo di certificazione**. L'adeguatezza delle misure si valuta in base alla natura, all'ambito, al contesto, alle finalità, probabilità e gravità dei rischi caratterizzanti l'ambito in cui si opera.

Il titolare pertanto deve **NON SOLO precostituire un apparato DOCUMENTALE** idoneo a garantire la protezione dai rischi dal punto di vista formale, **ma anche un apparato di misure FISICHE E ORGANIZZATIVE che proteggano effettivamente gli individui e i loro dati**.

Titolari e responsabili hanno l'obbligo di adottare comportamenti positivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

Si tratta di un'assoluta novità circa **l'autonomia e la possibilità di personalizzazione** delle procedure in capo a ciascun titolare/responsabile.

Si parla del concetto di **data protection BY DEFAULT and BY DESIGN**: vi è la necessità di configurare il trattamento prevedendo **fin dall'inizio** le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e, al tempo stesso, tutelare i diritti degli interessati tenendo conto del contesto e dei rischi specifici.

Assume **importanza la specifica previsione dei rischi**, che dovrà essere analizzata tramite la **valutazione di impatto privacy (DPIA) e assicurata dalla tenuta di un registro dei trattamenti.**

L'intervento dell'Autorità di controllo sarà ex post e si collocherà successivamente rispetto alle determinazioni assunte dal titolare: si assiste ad un'*abolizione della notifica preventiva dei trattamenti e del prior checking*.

I SOGGETTI

Il Regolamento protegge le persone fisiche

I) nel momento in cui **vengono trattati** i loro dati personali

II) nel momento in cui **circolano** i loro dati personali (art. 1).

E si applica a trattamenti **in tutto o in parte automatizzati, ma anche a quelli NON automatizzati** (art. 2).

Non si applica, come già in passato, in alcuni casi tassativamente previsti dall'art. 2….. ad esempio per attività a carattere **esclusivamente personale o domestico**….**o ai trattamenti effettuati dalle autorità competenti a fine di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali**…..

INTERESSATI – Art. 4 n. 1 Reg.:

Art. 4 n. 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.

Persone alle quali i dati si riferiscono con riferimento ad uno studio professionale: clienti, colleghi, collaboratori, dipendenti, fornitori tra cui consulenti.

TITOLARE DEL TRATTAMENTO – Art.4 n. 7 Reg.:

Art. 4 n. 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.

La figura del titolare rimane sostanzialmente invariata rispetto a quella prevista nel D. Lgs. 196/2003, in quanto egli **continua ad esercitare le stesse funzioni, ossia il potere decisionale** in ordine al trattamento.
Nel codice previgente era definito come *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"* (art. 4 lett. f Codice privacy).

Negli Studi legali e più in generale negli Studi Professionali il titolare del trattamento è:

- attività svolta individualmente → Avvocato o professionista in prima persona
- attività svolta congiuntamente → entrambi i professionisti ovvero i contitolari
- attività svolta in forma associata → il titolare è la società nel suo complesso.

Tale figura ha l'obbligo **(art. 24)** di:

- **adottare** misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato in modo conforme al regolamento; **le misure devono essere riesaminate e aggiornate**;
- aderire ai codici di condotta di cui all'art. 40 ovvero al meccanismo di certificazione di cui all'art. 42, al fine di dimostrare il rispetto degli obblighi facenti capo ad esso;
- mettere in atto fin dall'inizio (**art. 25 co.1**) misure tecniche e organizzative adeguate – pseudonomizzazione…minimizzazione - volte ad attuare in modo concreto i principi di protezione dei dati;
- mettere in atto (**art. 25 co. 2**) misure tecniche e organizzative adeguate per garantire che siano **trattati solo i dati personali necessari**, adottando procedure predefinite ed automatiche che garantiscano la giusta durata del trattamento dei dati e soprattutto il mancato accesso da parte di un numero indefinito di persone fisiche, non abilitate;
- curare il registro dei trattamenti svolti.

In particolare – adempimenti **di natura formale** richiesti al **titolare** del trattamento:

- Fornire l'informativa privacy – considerando 60 + Artt. 13/14 Reg.
- Acquisire il consenso o verificare altro presupposto di liceità – considerando 32 + Art. 6 Reg.
- Conferire apposite lettere di nomina
- Adottare le misure di sicurezza idonee alla protezione dei dati – considerando 83 + Art. 32 Reg.
- Effettuare eventuali notificazioni al Garante della Privacy – considerando 85 + Art. 33 Reg.

1. Fornire l'informativa

Considerando 60: i principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. Il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e del contesto specifici in cui i dati personali sono trattati. Inoltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa. In caso di dati personali raccolti direttamente presso l'interessato, questi dovrebbe inoltre essere informato dell'eventuale obbligo di fornire i dati personali e delle conseguenze in cui incorre se si rifiuta di fornirli. Tali informazioni possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone dovrebbero essere leggibili da dispositivo automatico.

VI E' OBBLIGO PER GLI STUDI PROFESSIONALI: Deve contenere gli elementi indicati negli artt. 13 e 14 Reg. Va fornita alle persone fisiche cui si riferiscono i dati trattati, **non solo ai clienti, ma anche ai dipendenti, ai collaboratori di Studio ed agli utenti del sito web. Nell'organizzazione dello studio l'Avvocato o comunque il professionista deve raccogliere i dati in modo lecito e secondo correttezza e la formazione del fascicolo può essere effettuata in via cartacea o mediante strumenti informatici**.

2. Acquisire il consenso o verificare altro presupposto di liceità

"***Considerando 32***: il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".

Art. 6 e ss. Reg. Il trattamento dei dati personali è ammesso solo con il consenso espresso liberamente dall'interessato, con riguardo ad un trattamento chiaramente individuato. È necessario che sia richiesto per iscritto, previa comunicazione dell'informativa.

Il professionista può trattare dati senza consenso quando **non sono facenti parte della categoria dei c.d. «dati sensibili» OGGI "PARTICOLARI"**. Non occorre chiedere il consenso dei clienti quando si tratta di dati «comuni» il cui trattamento è necessario per adempiere agli obblighi previsti dalla legge o derivanti dal contratto.

Inoltre, non occorre richiedere il consenso quando il trattamento dei dati sensibili è necessario per svolgere indagini difensive o per far valere o difendere un diritto in sede giudiziaria o stragiudiziale.

È bene ricordare che, in tal caso, il trattamento è legittimato da specifiche autorizzazioni del Garante della Privacy che riguardano le professioni forensi (Autorizzazioni del Garante Privacy 4/2016 + 7/2016).

Le condizioni di liceità del trattamento previste dall'art. 6 sono:

- consenso al trattamento;
- trattamento necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- trattamento necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Nel caso in cui le mail o i contatti dei clienti vengano utilizzate per inviare newsletter o servizi promozionali, è necessaria l'acquisizione di un consenso specifico.

3. Conferire apposite deleghe/ lettere di nomina

Il titolare deve nominare i soggetti autorizzati e i responsabili, con specifica indicazione dei compiti ad essi delegati.

All'interno di uno Studio, potrebbe essere utile identificare le seguenti figure:

- autorizzato alla reception/segreteria (anche indirizzamento e formazione fascicoli)
- autorizzato al controllo dei dati
- autorizzato alla registrazione e all'eventuale protocollo (se applicabile)
- autorizzato all'archiviazione
- autorizzato al controllo per la preparazione alla restituzione dei documenti

4. Adottare misure di sicurezza adeguate alla protezione dei dati

Considerando 83: Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un **adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere**. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

In osservanza del precedente Codice della Privacy era necessario predisporre misure di sicurezza adeguate a ridurre al minimo i rischi di distruzione, di perdita anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta (art. 31 e ss. del Codice).

A norma dell'art. 32 Reg., oggi, è necessario:

- aggiornare periodicamente le caratteristiche dell'individuazione dell'ambito del trattamento consentito agli autorizzati;

- prevedere procedure per un'idonea custodia di atti e documenti;

- prevedere procedure per la conservazione di determinati atti in archivi.

Le indicazioni di privacy suggerite dal CNF indicano di collocare i fascicoli in locali in cui non abbiano accesso diretto né clienti né terzi, quindi non nell'ingresso, nella sala d'aspetto o nei corridoi.

Nei locali in cui l'accesso è selezionato, gli autorizzati possono tenere e consultare i fascicoli attenendosi alle prescrizioni dell'ordinaria diligenza.

→ "*Per quanto riguarda l'organizzazione del lavoro quotidiano di studio, va osservato che, contrariamente a quanto ipotizzato in alcuni quesiti formulati da singoli professionisti,* ***non occorre depennare il nome delle parti dalla copertina dei fascicoli cartacei, utilizzando al suo posto solo numeri identificativi. Resta invece necessario seguire opportune modalità per rendere i fascicoli e la relativa documentazione accessibili agli autorizzati del trattamento nei casi e per le finalità previsti***" (Garante privacy, parere del 3 giugno 2004 reso al Consiglio nazionale forense).

Consigli per la gestione quotidiana dello Studio

In particolare, vi sono luoghi dello Studio che hanno maggior rilevanza nel trattamento dei dati:

- **reception/segreteria: è il luogo che, in assoluto, presenta il più alto rischio di violazione della privacy, in quanto è area esposta al pubblico ed agli interessati. Il rischio di interscambio di informazioni con terzi che non siano l'interessato è molto elevato.**
- **Non vi devono essere esposti documenti di terzi**, qualsiasi dato che venga trasferito agli autorizzati va posto in apposite cartellette. Se l'interessato desidera effettuare delle comunicazioni, è necessario che questo avvenga in sede separata. È importante che il fax non sia situato in questa stanza.
- sala riunioni: l'interessato, in questo caso, ha un rapporto diretto con il professionista. Non presenta rischi particolari. Bisogna evitare di tenervi fascicoli che non riguardino l'interessato.
- sala archivio: è bene proteggere con ogni cura tale stanza, in modo tale che nessuno, al di fuori del professionista e dei suoi collaboratori, vi abbia accesso. Sarebbe opportuno chiudere a chiave la stanza.

Misure di sicurezza attualmente in vigore

Per quanto riguarda le misure di sicurezza inerenti i trattamenti con l'ausilio di strumenti elettronici, è necessario:

- prevedere idonee procedure di autenticazione informatica;
- implementare sistemi di autorizzazione (password, user ID). Assegnare uno user ID personale a ogni autorizzato, predisporre e inserire una password da modificare ogni 6 mesi;
- aggiornare periodicamente i software;
- proteggere gli strumenti elettronici e i dati rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici;
- provvedere a strutturare procedure per custodia di copie di sicurezza e ripristino della disponibilità dei dati;
- installare antivirus adeguati.

È consigliabile procedere ad aggiornare spesso le password. L'elenco delle medesime va conservato dal titolare del trattamento e possono avervi accesso solo i dipendenti e i collaboratori dello Studio.

Non è da trascurare la problematica relativa al trasferimento dei dati al di fuori dell'Unione Europea. Per quanto potrebbe sembrare superfluo, in realtà l'utilizzo di servizi quali Google Drive, Dropbox o Icloud rappresentano veri e propri veicoli di dati all'estero. Pertanto, è necessario che anche tale eventualità venga prevista e citata nell'informativa.

In sostituzione del DPS → REGISTRI DEI TRATTAMENTI – considerando 82 + art. 30 Reg.:

*"**Considerando 82:** per dimostrare che si conforma al presente regolamento, **il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento** effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti".*

Art. 30: Tutti i titolari e i responsabili dei trattamenti, devono tenere, separatamente, un registro delle operazioni di trattamento (**tranne – art. 30 co. 5 Reg. - in organismi con meno di 250 dipendenti, a meno che effettuino trattamenti a rischio per i diritti e le libertà dell'interess., il tratt. non sia occasionale, abbia ad ogg. dati particolari di cui all'art. 9 par. 1; ovvero dati pers. Relativi a condanne penali e reati ex art. 10**) → quadro aggiornato dei trattamenti da tenere a disposizione di eventuali controlli.

È importante sottolineare come non si tratti solo di un adempimento formale, bensì della parte integrante di un sistema di corretta gestione dei dati personali.

Come Professionisti riteniamo utile dotarsi dei registri dei trattamenti anche nelle realtà minori, per quanto non sia obbligatorio. I registri compongono l'apparato documentale da tenere a disposizione per dimostrare la propria conformità alla normativa.

5. Effettuare eventuali notificazioni al Garante della Privacy:

Considerando 85: **una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare** danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. **Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.** Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Precedentemente, l'art. 37 Codice Privacy si occupava dell'onere di notificazione preventiva.

Con l'entrata in vigore del Regolamento, ex art. 33, occorre effettuare la notificazione al Garante solo in caso di *data breach*, ossia di violazione dei dati personali. Nel caso in cui si verifichi detta eventualità il titolare del trattamento deve notificare la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza.

RESPONSABILE DEL TRATTAMENTO – Considerando 81 + Art. 4 n. 8 Reg. e art. 28 Reg.:

Considerando 81: Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, **quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento**.

L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento.

L'esecuzione dei trattamenti da parte di un responsabile del trattamento dovrebbe essere disciplinata 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, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato.

Il titolare del trattamento e il responsabile del trattamento possono scegliere di usare un contratto individuale o clausole contrattuali tipo che sono adottate direttamente dalla Commissione oppure da un'autorità di controllo in conformità del meccanismo di coerenza e successivamente dalla Commissione.

Dopo il completamento del trattamento per conto del titolare del trattamento, il responsabile del trattamento dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione dei dati personali.

La designazione è facoltativa. Si tratta della *"persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*.

Rispetto al Codice previgente, oggi il titolare del trattamento deve predisporre un idoneo contratto scritto o altro atto giuridico similare che, oltre a vincolare reciprocamente le due figure, deve prevedere la materia disciplinata, la durata del trattamento, la natura e le finalità del medesimo nonché la tipologia di dati personali e le categorie di interessati a cui gli stessi dati si riferiscono.

In capo al Responsabile del Trattamento vi sono diversi obblighi:

- non ricorrere ad altro responsabile senza autorizzazione del titolare;
- disciplinare i trattamenti dati con un contratto o con un atto giuridico che vincoli il responsabile in quanto a durata, finalità e natura del trattamento, nonché gli obblighi e i diritti del titolare di trattamento;
- non trattare i dati senza il consenso e le istruzioni del titolare.

E' consentita la nomina di sub-responsabili del trattamento per specifiche attività, nel rispetto degli obblighi contrattuali che legano il titolare ed il responsabile primario.

Il responsabile del trattamento deve curare la tenuta del registro dei trattamenti svolti (ove applicabile), adottare misure tecniche e organizzative per garantire la sicurezza.

RESPONSABILE PROTEZIONE DATI/DATA PROTECTION OFFICER (RPD/DPO) – Considerando 77 + Art. 37 Reg.

Considerando 77: Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato **o indicazioni fornite da un responsabile della protezione dei dati**. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio.

Si tratta di un soggetto che ha conoscenza specialistica della normativa e delle pratiche in materia di protezione dati: fornisce assistenza al titolare e al responsabile del trattamento dati, che sono i soggetti tenuti a nominarlo in particolari situazioni.

Vige l'obbligo di nomina se:

- **il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni;**
- **le attività principali** consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, **richiedono il monitoraggio regolare e sistematico degli interessati su larga scala** (i fattori che connotano un trattamento su larga scala, individuati dai garanti europei, sono: il numero di soggetti interessati dal trattamento, in termini assoluti o in percentuale; il volume dei dati e la loro tipologia, la durata o la persistenza dell'attività di trattamento; la portata geografica dell'attività di trattamento);
- **se le attività principali consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10.**

In ogni caso, il DPO può sempre essere facoltativamente nominato.

- **La scelta dev'essere effettuata in base alle qualità professionali. Può trattarsi di un dipendente del titolare o del responsabile oppure un soggetto esterno legato al titolare/responsabile da un contratto di servizi.**

Il suo nominativo va segnalato al garante.

Negli Studi legali, vige l'obbligo di nomina del DPO nel caso in cui le attività principali consistano nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10 Linee Guida del Gruppo di lavoro art. 29 (WP29).

Occorre, però, tener conto di vari fattori (numero di soggetti interessati dal trattamento, volume dei dati e/o loro diversa tipologia, durata o persistenza dell'attività di trattamento, portata geografica dell'attività di trattamento).

Non si considera su larga scala il "trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato".

Il DPO in sintesi….

Il DPO deve:

- informare e fornire consulenza al titolare o al responsabile, nonché formare i dipendenti;
- sorvegliare sull'osservanza del Regolamento;
- fornire parere in merito alla valutazione di impatto sulla protezione dei dati;
- fungere da organo di cooperazione con l'Autorità di controllo;
- inviare periodicamente comunicazioni, promuovere iniziative e eventi di aggiornamento e approfondimento sul tema.

Il Gruppo di lavoro art. 29 suggerisce di stipulare un contratto dotato di apposite clausole:

- **il DPO dev'essere invitato a partecipare alle riunioni;**
- **la presenza del DPO è obbligatoria ogni qualvolta debbano essere assunte decisioni che abbiano impatto sulla protezione dei dati, al fine di permettergli di fornire idonea consulenza;**
- **dev'essere garantita una consultazione tempestiva qualora si verifichi una violazione del trattamento dei dati;**
- **dev'essere fornito al DPO supporto adeguato in termini di risorse finanziarie.**
- **Il DPO non è direttamente responsabile in caso di inosservanza degli obblighi in materia di protezione dati: spetta al titolare o al responsabile garantire che il trattamento sia effettuato conformemente al regolamento.**

Autorizzati del trattamento

rispetto al Codice Privacy previgente, in cui gli incaricati erano "*le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile*" (art. 4 lett. h Codice privacy), nel regolamento UE non vi è una definizione espressa di incaricati

Di fatto, però, coincidono con "*le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*", richiamate in alcune disposizioni.

In concreto, possono essere designati dei «soggetti deputati» alla privacy all'interno dello Studio, così come altri responsabili, soggetti esterni.

In ogni caso, chiunque abbia accesso ai dati deve essere espressamente designato quale autorizzato del trattamento (segreteria, personale amministrativo, colleghi, praticanti, responsabile informatico).

-

A tal proposito, è importante il concetto di formazione del personale tramite corsi o workshop.

PROCEDURE DI TUTELA: IMPORTANTE E INTERESSANTE

Le procedure di tutela sono previste dagli artt. 77/84 Regolamento, unitamente al considerando 141.

L'interessato può conferire delega per reclami, ricorsi e richieste di risarcimento a enti come organizzazioni o associazioni senza scopo di lucro che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione di dati personali.

Considerando 141: **ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo**, in particolare nello Stato membro in cui risiede abitualmente, **e il diritto a un ricorso giurisdizionale** effettivo a norma dell'articolo 47 della Carta **qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato**. **Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico. È opportuno che l'autorità di controllo informi gli interessati dello stato e dell'esito del reclamo entro un termine ragionevole**. Se il caso richiede un'ulteriore indagine o il coordinamento con un'altra autorità di controllo, l'interessato dovrebbe ricevere informazioni interlocutorie. **Per agevolare la proposizione di reclami, ogni autorità di controllo dovrebbe adottare misure quali la messa a disposizione di un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione**.

LA TUTELA INNANZI AL GARANTE – art. 77 Reg.

Il Garante per la protezione dei dati personali è un'**Autorità indipendente** che, nelle intenzioni del legislatore, dovrebbe operare in piena **autonomia** e con **indipendenza** di giudizio e di valutazione.

COMPITI DEL GARANTE:

Vecchia normativa: art. 154 Codice Privacy

- controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile in conformità alla notificazione, anche in caso di loro cessazione;
- esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;
- prescrivere, anche d'ufficio, ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143;
- vietare anche d'ufficio, in tutto o in parte, il trattamento illecito e non corretto dei dati o disporre il blocco ai sensi dell'art. 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;

(segue)

- promuovere la sottoscrizione di codici ai sensi dell'articolo 12 e dell'art. 139;
- segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti di cui all'articolo 2 anche a seguito dell'evoluzione del settore;
- esprimere pareri nei casi previsti;
- curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati;
- denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza dell'esercizio o a causa delle funzioni;
- tenere il registro dei trattamenti formato sulla base di notificazioni di cui all'articolo 37.
- predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione delle norme previste dal codice, che è trasmesso al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.

Nuova normativa: art. 57 GDPR – Focus di Autorità di controllo

1. Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo:

- a) sorveglia e assicura l'applicazione del presente regolamento;
- b) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;
- c) fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;
- d) promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;
- e) **su richiesta, fornisce informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dal presente regolamento e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri**;

f) **tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 80, e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole**, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;

g) **collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento**;

h) **svolge indagini sull'applicazione del presente regolamento**, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;

i) **sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali**;

j) adotta le clausole contrattuali tipo di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);

k) **redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4**;

l) **offre consulenza sui trattamenti** di cui all'articolo 36, paragrafo 2 (**consultazione preventiva**);

m) **incoraggia l'elaborazione di codici di condotta** ai sensi dell'articolo 40, paragrafo 1, e **fornisce un parere su tali codici di condotta e approva quelli che forniscono garanzie sufficienti**, a norma dell'articolo 40, paragrafo 5;

n) **incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati** a norma dell'articolo 42, paragrafo 1, e approva i criteri di certificazione a norma dell'articolo 42, paragrafo 5;

o) ove applicabile, effettua **un riesame periodico delle certificazioni** rilasciate in conformità dell'articolo 42, paragrafo 7;

p) **definisce e pubblica i criteri per l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43**;

q) **effettua l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43**;

r) **autorizza le clausole contrattuali** e le altre disposizioni di cui all'articolo 46, paragrafo 3;

s) approva le norme vincolanti d'impresa ai sensi dell'articolo 47;

t) contribuisce alle attività del comitato;

u) **tiene registri interni delle violazioni del presente regolamento e delle misure adottate in conformità dell'articolo 58, paragrafo 2**; e

v) svolge qualsiasi altro compito legato alla protezione dei dati personali.

2. **Ogni autorità di controllo agevola la proposizione di reclami di cui al paragrafo 1, lettera f), tramite misure quali un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione**.

3. **Ogni autorità di controllo svolge i propri compiti senza spese né per l'interessato né, ove applicabile, per il responsabile della protezione dei dati.**

4. Qualora le richieste siano manifestamente infondate o eccessive, in particolare per il carattere ripetitivo, l'autorità di controllo può addebitare un contributo spese ragionevole basato sui costi amministrativi o rifiutarsi di soddisfare la richiesta. Incombe all'autorità di controllo dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

STRUMENTI: RECLAMO, SEGNALAZIONI, RICORSI

L'art. 77 GDPR prevede il diritto di proporre **reclamo** all'autorità di controllo, nello Stato membro in cui risiede oppure nel luogo in cui si è verificata la presunta violazione. Vi sono altresì riferimenti alle **segnalazioni**, e una regolamentazione dello strumento del **ricorso**.

Anche il Codice privacy prevedeva la **tutela innanzi all'Autorità Garante,** cui l'interessato poteva rivolgersi (secondo quanto disposto dall'art. 141):

1) Mediante un **reclamo circostanziato** per rappresentare una violazione delle norme in materia di trattamento dei dati personali;

2) Mediante una **segnalazione** al fine di sollecitare un controllo da parte del Garante sulla medesima disciplina;

3) Mediante un **ricorso**, se intende far valere gli specifici diritti che l'art. 7 gli riconosce e garantisce

1. Reclamo

Codice privacy

Il Codice privacy, invece, prevede (meglio, prevedeva) che questo dovesse contenere:

- indicazione dettagliata dei fatti e delle circostanze su cui si fonda;
- indicazione delle disposizioni che si presumono violate;
- indicazione delle misure richieste;
- estremi identificativi del titolare, del responsabile, ove conosciuti e, ovviamente, dell'istante stesso.

Nel reclamo doveva essere indicato anche l'indirizzo di posta elettronica, di telefax o di telefono cui si intende ricevere le relative comunicazioni e può essere corredato da un apposito allegato con la documentazione utile ai fini del decidere.

L'atto doveva essere **sottoscritto dall'interessato** o, eventualmente, dalle associazioni che lo rappresentano.

Il Garante, infine, poteva predisporre un modello *ad hoc* per il reclamo e di cui doveva favorire la disponibilità con strumenti elettronici. La normativa in via di superamento considerava **Internet il canale principale** attraverso il quale diffondere servizi come, in questo caso, il *fac simile* per predisporre un reclamo.

Presentato il reclamo ed esaurita la dovuta conseguente istruttoria preliminare, se non è manifestamente infondato, e sussistono i presupposti per adottare un provvedimento, può cercare di **addivenire ad una soluzione amichevole della controversia** invitando il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente.

In caso contrario il Garante può:

- prescrivere al titolare misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;
- disporre il blocco o vietare, in tutto o in parte, il trattamento che risulta illecito, o non corretto, anche per effetto della mancata adozione delle misure necessarie da esse stessa impartite.

Il Garante può anche vietare in tutto o in parte il trattamento dei dati relativi a singoli soggetti o a categorie di soggetti quando si ponga in contrasto con rilevanti interessi della collettività.

Reclamo ai fini del GDPR

Per il **reclamo** non sono previste particolari formalità, il GDPR non menziona alcunché circa il suo contenuto.

Ai sensi dell'art. 77 comma 2, l'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78. Ai sensi del considerando 141, ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo, in particolare nello Stato membro in cui risiede abitualmente, e il diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato. Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico.

È opportuno che l'autorità di controllo informi gli interessati dello stato e dell'esito del reclamo entro un termine ragionevole. Se il caso richiede un'ulteriore indagine o il coordinamento con un'altra autorità di controllo, l'interessato dovrebbe ricevere informazioni interlocutorie. Per agevolare la proposizione di reclami, ogni autorità di controllo dovrebbe adottare misure quali la messa a disposizione di un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione.

2. Segnalazioni

Codice Privacy

Un sola norma – l'art. 144 - è dedicata dal codice alle segnalazioni. In particolare, i provvedimenti che il garante emana a seguito di un reclamo possono essere adottati anche a seguito di una segnalazione purché sia stata avviata un'istruttoria preliminare e anche prima della definizione del procedimento. Peraltro l'art. 144 non trova alcun immediato referente normativo un'atra disposizione previgente.

GDPR

Nell'ambito del GDPR, le segnalazioni sono citate ma non regolamentate, pertanto si ritiene che, in materia, possa essere ancora applicabile il Codice Privacy.

3. Ricorso

Il GDPR fa riferimento al solo RICORSO **GIURISDIZIONALE**, anche avverso le decisioni giuridicamente vincolanti del Garante.

Pertanto, sarebbe opportuno attendere l'adeguamento della normativa interna al fine di comprendere se la disciplina del ricorso prevista dagli artt. 145 e seguenti del Codice della Privacy sarà ancora applicabile.

RESPONSABILITA' CIVILE PER DANNI – art. 82 Reg. Considerando 146

Preliminarmente, va ricordato che il titolare si espone innanzitutto ad una responsabilità civile, laddove cagioni un danno per effetto del trattamento dei dati: trattasi di responsabilità di cui all'articolo 2050 c.c., per esercizio di attività pericolosa. Chiunque subisca un danno causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno, patrimoniale e non, dal titolare o dal responsabile del trattamento (qualora quest'ultimo non abbia adempiuto agli obblighi specificatamente a lui diretti). A norma dell'art. 82 Regolamento, l'accusato deve provare la propria innocenza (inversione onere della prova).

Occorre in ogni caso inquadrare l'atto o l'omissione illecita quale violazione di una specifica prescrizione del Regolamento.

- I rischi che possono dar luogo a risarcimento si configurano se il trattamento:
- cagioni un danno fisico, materiale o immateriale;
- comporti discriminazioni, furto, usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto, decifratura non autorizzata della pseudonimizzazione, diffusioni di dati su origine razziale o etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, salute, vita sessuale, condanne penali, reati.

La responsabilità civile è solidale tra le due figure. Ciascuno risponde per l'intero ammontare, salvo azione di rivalsa. Per intraprendere eventuali azioni di rivalsa occorre verificare se:

- il titolare ha impartito istruzioni al responsabile;
- le istruzioni erano specifiche o generiche;
- il responsabile le ha disattese;
- il titolare ha verificato che il responsabile fosse in grado di eseguire le istruzioni;
- il responsabile ha assunto obblighi che era in grado di assolvere;
- il titolare ha effettuato verifiche periodiche;
- il responsabile ha avvisato il titolare di istruzioni illegittime;
- ci sono clausole di ripartizione della responsabilità.
- L'adesione a codici di condotta e certificazione non garantiscono l'esonero di responsabilità.

SANZIONI AMMINISTRATIVE – Art. 83 Reg.

Disciplina previgente: una serie di **sanzioni amministrative di tipo pecuniario** erano previste in particolare nel **Capo I del Titolo III della Terza Parte del codice** in caso di:

- omessa o inidonea informativa all'interessato;

- illecita cessione dei dati;

- omessa o incompleta notificazione;

- omessa informazione o esibizione al Garante.

L'**articolo 161** puniva le ipotesi di **omessa o inidonea informativa all'interessato**, cioè quelle condotte tenute in violazione dell'art. 13 del Codice per aver completamente omesso di adempiere all'obbligo dell'informazione, o per aver proceduto a tale adempimento in modo sostanzialmente inidoneo rispetto alle modalità e alle finalità previste della legge.

L'art. 162 puniva, con una sanzione che varia da diecimila e sessantamila euro, l'**illecita cessione di dati** e le violazioni delle **disposizioni in materia di disciplina del trattamento dei dati personali.**

Al secondo comma, puniva poi la violazione della disposizione di cui all'articolo 84, primo comma, in tema di comunicazione dei dati idonei a rilevare lo stato di salute.

Quanto alle possibili violazioni delle norme in tema di notificazione, l'art 163 puniva "chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi dell'articolo 37 e 38, ovvero indica in essa notizie incomplete". In realtà il termine "chiunque" appare inadeguato potendo commette tale illecito solo chi abbia l'obbligo giuridico di procedere alla notificazione: ovvero al titolare del trattamento.

Infine, l'art. 164 puniva "chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ".

Per tutte le violazioni amministrative poteva essere applicata **la sanzione accessoria della pubblicazione dell'ordinanza - ingiunzione**, per intero o per estratto, in uno o più giornali.

Per tutte le ipotesi appena citate l'art. 164 bis del Codice prevedeva che i limiti massimi e minimi delle sanzioni potessero essere applicati in misura pari a due quinti se il fatto era di **minore gravità**; per valutare la gravità si aveva riguardo alla natura anche economica e sociale dell'attività svolta.

Lo stesso art. 164 bis prevedeva alcune ipotesi aggravate molto severe in caso di una o più violazioni di un'unica o più disposizioni, commesse anche in tempi diversi in relazione a banche dati di particolare rilevanza o dimensioni.

I limiti minimo e massimo delle sanzioni erano raddoppiati in altri casi di maggiori gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolgeva numerosi interessati.

Infine le sanzioni potevano essere aumentate fino al quadruplo quando potevano risultare inefficaci in ragione delle condizioni economiche del contravventore.

Quanto al procedimento di applicazione delle sanzioni amministrative, l'art.166 riconosceva la competenza al Garante e disponeva l'applicazione delle norme di cui alla legge 689/1981.

Il GDPR, a differenza della disciplina previgente, individua gli importi e le circostanze in cui possono essere comminate le sanzioni amministrative, con particolare riferimento alle sanzioni amministrative pecuniarie massime per specifiche violazioni del Regolamento, che vengono elencate in maniera puntuale, e ai nuovi criteri per la ponderazione della sanzione pecuniaria inerenti a tutte le contingenze che attengono alla situazione concreta, tra cui la natura, la gravità, la durata dell'infrazione e le relative conseguenze.

Le sanzioni sono distinte in base al tipo di violazione. In caso di mera violazione degli obblighi da parte del titolare o del responsabile del trattamento si arriva ad un massimo di 10 milioni di € o del 2% del fatturato dell'impresa.

Se, invece, vi è una violazione dei diritti degli interessati, il limite si innalza fino a 20 milioni di € o al 4% del fatturato dell'impresa.

Il Garante può rivolgere avvertimenti al titolare o al responsabile del trattamento sul fatto che i trattamenti previsti possano violare le disposizioni.

Egli può rivolgere ammonimenti o infliggere una sanzione amministrativa pecuniaria in funzione del singolo caso, parametrata alla dimensione dell'azienda.

Importo sanzione per più violazioni → l'importo totale non può superare l'importo specificato per la violazione più grave.

Concetto di dolo e colpa

- Possiamo fare riferimento ai concetti tradizionali di dolo e di colpa.
- Una violazione è dolosa quando è prevista e voluta.
- E' colposa quando è la conseguenza di un comportamento negligente ed imprudente ovvero conseguenza di imperizia laddove questa è richiesta; oppure quando è conseguenza della violazione di leggi, regolamenti, ordini, discipline, prassi e linee guida.

Il sistema sanzionatorio viene radicalmente innovato dal Regolamento:

- innalzamento rilevante dell'importo delle sanzioni;
- alternatività sanzioni pecuniarie e ammonizione;
- inserimento della violazione di tutti i principi e tutti gli obblighi tra gli illeciti amministrativi.

Elementi utilizzati per la valutazione, ai fini dell'irrogazione della sanzione:

- **Natura, gravità e durata violazione: nei casi in cui la violazione sia "minore" e non crei un rischio significativo per i diritti degli interessati, la sanzione può essere sostituita con un ammonimento**.
- **Abbiamo una struttura a livelli dell'apparato sanzionatorio. La natura della violazione, l'oggetto o la finalità del trattamento, nonché il numero di interessati lesi dal danno e il livello del danno da essi subito forniranno un'indicazione della gravità della violazione. Se gli interessati hanno concretamente subito un danno, occorre considerarne l'entità (considerando 75).**

- **Carattere doloso o colposo della violazione**: il dolo consiste negli elementi di consapevolezza e intenzionalità (es. volontaria modifica di dati personali per dare un'impressione fuorviante circa il conseguimento degli obiettivi, caso di un ospedale che aveva modificato i dati per far risultare un accesso in struttura superiore al reale; vendita di dati personali con finalità di marketing) . **La colpa consiste nella violazione di un obbligo di diligenza (errore umano, incapacità di approntare aggiornamenti tecnici, mancata verifica della correttezza dei dati pubblicati**).

- **Misure adottate per attenuare il danno subito dagli interessati**: quando si verifica una violazione, la parte responsabile dovrebbe fare quanto in suo potere per ridurre le conseguenze della violazione per i soggetti coinvolti. La loro adozione viene valutata come attenuante o aggravante.

- **Grado di responsabilità di titolare e responsabile del trattamento, tenendo conto delle misure tecniche e organizzative messe in atto ai sensi degli artt. 25 e 32**: titolari e responsabili devono tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. È importante tenere conto dei codici di condotta.

- **Eventuali violazioni precedenti, pertinenti, commesse da titolare o responsabile**

- **Grado di cooperazione con Autorità di controllo al fine di porre rimedio alla violazione e attenuare possibili effetti negativi**.
- **Categorie di dati interessati dalla violazione. Stabilire quali danni e disagi si sono causati al soggetto coinvolto e se si tratta dei dati particolari menzionati agli artt. 9 e 10 Reg**.
- **Notificazione della violazione: verificare la sua eventuale presenza e in che modo l'autorità è venuta a conoscenza della violazione. Il titolare ha l'obbligo di notificare alle Autorità eventuali violazioni di dati**.
- **Rispetto di eventuali prescrizioni imposte precedentemente in merito allo stesso tipo di violazioni.**
- **Adesione a codici di condotta o meccanismi di certificazione**.
- **Eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, come benefici finanziari conseguiti o perdite evitate quale conseguenza della violazione**.

Sanzioni afflittive:

Fino a 10 milioni di Euro, o per le imprese, fino al 2% del fatturato annuo mondiale dell'esercizio precedente, nei casi di:

- inosservanza degli obblighi del titolare e del responsabile del trattamento;
- inosservanza degli obblighi dell'organismo di certificazione;
- inosservanza degli obblighi dell'organismo di controllo.

Fino a 20 milioni di Euro, o per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente, nei casi di:

- inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati;
- inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali;
- inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo. Inosservanza di un ordine correttivo dell'autorità di controllo.

Sanzioni correttive:

Le sanzioni correttive sono connesse ai poteri dell'Autorità di controllo, la quale può:

- **rivolgere avvertimenti** al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR;
- **rivolgere ammonimenti** al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR;
- **ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti**;
- **ingiungere al titolare o al responsabile del trattamento di conformare i trattamenti alle disposizioni del GDPR, anche specificando in che modo ed entro quale termine**;
- **ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali**;
- **imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento**;

- **Ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali;**
- **Revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;**
- **Infliggere una sanzione amministrativa pecuniaria in aggiunta alle presenti misure;**
- **Ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.**

SANZIONI PENALI

Il Regolamento non contiene disposizioni volte a disciplinare direttamente la responsabilità penale che deriva dall'illecito trattamento dei dati personali, tuttavia i singoli Stati membri hanno la possibilità di prevedere sanzioni di carattere penale, poiché il Legislatore europeo ha espressamente demandato la scelta del regime relativo alla responsabilità penale agli Stati stessi.

Le principali disposizioni di riferimento, afferenti al novero delle fonti normative della materia, sono il Considerando n. 149 e l'art. 84 del *GDPR*, da combinarsi insieme con l'art. 83.2 TFUE.

Il Considerando n. 149, infatti, sancisce che i singoli Stati debbano poter stabilire le disposizioni concernenti le sanzioni penali applicabili in caso di violazione del Regolamento e in caso di violazione delle norme nazionali adottate in virtù ed entro i limiti posti dal Regolamento.

È, altresì, ammesso che le sanzioni aventi carattere penale, previste dagli Stati membri, possano implicare la sottrazione dei profitti ricavati mediante la violazione del Regolamento, a condizione che venga rispettato il principio del *ne bis in idem*, quale interpretato dalla Corte di Giustizia europea.

Per quanto attiene alla legislazione interna, risultano, dunque, compatibili con la nuova normativa europea le previsioni sulla responsabilità penale di cui al Decreto legislativo. n. 196/2003 (*cfr.* Codice in materia di protezione dei dati personali).

Ad oggi, infatti, il Codice della privacy prevede che la responsabilità penale possa derivare da alcune specifiche condotte, le quali, ai sensi dell'articolo 167 Codice privacy, devono essere volte a trarre profitto, per sé o per altri, oppure ad a cagionare danno e devono aver arrecato nocumento al soggetto danneggiato, sempre salvo il caso in cui il fatto costituisca un più grave reato secondo la legge.

Il legislatore prevede delle ipotesi di reato conseguenti a particolari condotte tenute in violazione delle norme del Codice.

Il reato di **trattamento illecito dei dati**, previsto dall'art. 167, punisce la condotta di chiunque al fine di trarre per sé o per altri profitto, o di recare ad altri un danno, procede al trattamento dei dati personali in violazione delle norme dettate in tema di principi applicativi a tutti i trattamenti effettuati da soggetti pubblici, ovvero in tema di principi applicabili a tutti i trattamenti di dati diversi da quelli sensibili e giudiziari, o ancora in tema di consenso, ovvero infine in tema di dati relativi al traffico, dati relativi all' ubicazione, comunicazioni indesiderate o elenchi di abbonati.

In tale ampia previsione, il legislatore non specifica il tipo di profitto – ovvero se lo stesso debba essere ingiusto - né il tipo di danno patrimoniale o anche non patrimoniale ma richiede per l'effettiva punibilità che **dal fatto derivi un nocumento**. La pena e quella della reclusione de sei mesi a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, quella della reclusione da sei a ventiquattro mesi.

E' punita la condotta di " chiunque" al fine di recare per sé o per altri profitto o di recare ad altri danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45".

Le norme richiamate sono quelle dettate in tema di **trattamento che presenta rischi specifici, di principi applicabili al trattamento di dati sensibili, di principi applicabili al trattamento di dati giudiziari, di principi applicabili al trattamento di dati sensibili e giudiziari**, ovvero ancora in tema di divieti di comunicazione e diffusione, di garanzie per i dati sensibili, di garanzie per i dati giudiziari e infine di trasferimenti vietati all'estero. La sanzione prevista è la reclusione da uno a tre anni se dal fatto deriva nocumento e salvo che il fatto costituisca più grave reato.

Il reato di **falsità nelle dichiarazioni e notificazioni al Garante** è previsto dall'art. 168 che punisce, con la reclusione da 6 mesi a 3 anni, chiunque nella notificazione o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento innanzi al Garante o nel ricorso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi.

Tale fattispecie, che opera con la clausola " salvo che costituisca più grave reato", può ascriversi alla categoria dei **reati comuni**; benché infatti la notificazione di cui all'art. 37 sia un obbligo che incombe solo sul titolare del trattamento, la portata della norma è così ampia da ricomprendere anche condotte che possono validamente essere posti in essere da "chiunque".

L'art.169 punisce con l'arresto sino a due anni chi essendovi tenuto, **omette di adottare le misure minime di sicurezza** previste dall'articolo 33.

Tale reato omissivo è un reato proprio perché può essere contestato soltanto a chi per legge sia tenuto ad adottare le misure di sicurezza ovvero al titolare del trattamento.

Il legislatore prevede in particolare **cause di estinzione del reato.**

Invero, al soggetto attivo, all'atto dell'accertamento – ovvero nei casi di particolare complessità, anche con atto successivo del Garante – viene impartita una prescrizione in cui si fissa un termine per la regolarizzazione che non ecceda il periodo di tempo tecnicamente necessario (peraltro probabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi). Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la sanzione amministrativa.

L'adempimento e il pagamento estinguono il reato.

Infine altre prescrizioni puniscono l'inosservanza di taluni provvedimenti del Garante, come le violazioni in tema di pertinenza dei dati raccolti dal datore di lavoro, ovvero di controllo a distanza dei lavoratori stessi.

La regola comune delle diverse fattispecie di reato ora esaminate è la pena accessoria della pubblicazione della sentenza di condanna prevista, per i soli delitti, dall'art. 172.

L'art. 171 espressamente prevede che la violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

Le violazioni da parte del datore di lavoro in tema di divieto di svolgere indagini sulle convenzioni, adesioni e opinioni religiose, filosofiche, politiche etc. del lavoratore, nonché in tema di controlli a distanza, sono punite con la sanzione prevista dall'art. 38 dello Statuto dei lavoratori.

Orbene, l'art 38 cit. prevede le sanzioni dell'arresto e dell'ammenda ragion per cui configura una fattispecie di contravvenzione alla quale applica anche – nei casi più gravi – la pubblicazione della sentenza penale di condanna.

Quindi, a seguito del rechiamo effettuato dal codice a tale previsione, o meglio a tali sanzioni previste dallo Statuto del lavoratori , abbiamo una fattispecie di reato contravvenzionale cui si può applicare anche la pubblicazione della sentenza di condanna quando invece lo stesso codice limita tale possibilità alle figure delittuose.

La domanda che ci si può porre è se e in che misura tali norme sanzionatorie penali continuino a restare in vigore e a non essere abrogate.

La risposta non può essere data in senso univoco, dal momento che talune disposizioni del Codice della privacy, la cui violazione configurava finora una fattispecie di reato richiamata nella norma penale, potrebbero essere considerate abrogate per incompatibilità rispetto al *GDPR*, mentre altre potrebbero rimanere perfettamente valide.

In ogni caso si ritiene che il sistema sanzionatorio penale manterrà delle fattispecie di applicabilità