Ordine dei Dottori Commercialisti
e degli Esperti Contabili di Benevento

Regolamento privacy UE 2016/679: impatto sugli studi professionali, accountability e obbligo di nomina del Data Protection Officer per le aziende

BENEVENTO – 19 MAGGIO 2018

Graziano Garrisi - UniSalento
Responsabile della Protezione dei Dati dell'ODCEC di Lecce
Responsabile Gruppo di ricerca «Privacy e Data Protection» del MODiCT
Avvocato esperto in Diritto delle nuove tecnologie

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE:

- **abroga la vecchia direttiva 95/46/CE, recepita nei vari Stati membri e anche nel nostro ordinamento con il d.lgs. 196 del 2003 (Codice Privacy)**
- **non semplificherà l'attuale disciplina né ridurrà gli oneri a carico dei titolari del trattamento, al contrario introdurrà nuovi adempimenti e differenti modelli organizzativi**
- **la maggior parte dei provvedimenti del Garante resterà valida ed efficace**
- **Esecutività (Regolamento): 2 anni da entrata in vigore (= 25 maggio 2018)**

173 Considerando

99 Articoli

Regolamento UE n. 2016/679

Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati

(Regolamento generale sulla protezione dei dati)

La Commissione Europea considera il regolamento europeo, in quanto **self-executing**, come lo strumento più idoneo per definire il quadro giuridico per la protezione dei dati personali nell'UE. In quanto l'applicabilità diretta del regolamento negli Stati membri ridurrà la frammentazione giuridica e offrirà maggiore certezza giuridica, migliorando la tutela dei diritti fondamentali delle persone fisiche e contribuendo al corretto funzionamento del mercato interno.

Accountability:
conta dimostrare la sostanza degli adempimenti e delle misure di sicurezza senza inutili formalismi

Il titolare del trattamento deve essere in grado di dimostrare che ha adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, attraverso l'elaborazione di specifici modelli organizzativi (analoghi a quelli del d. lgs. 231/2001):

approccio basato sulla valutazione del rischio che premia i soggetti più responsabili (azione preventiva/proattiva e non reattiva)

E' una declinazione del verbo **«dimostrare»**: Studi professionali e singoli professionisti devono sviluppare e dotarsi di strumenti che possano essere utilizzati per valutare lo stato della propria accountability per dimostrarlo all'Autorità Garante.

Decadenza della figura dell'incaricato, aggiunta dei contitolari **Art. (4, 26)**	**Modifica dei punti obbligatori nelle informative** **Art. (14)**	**Introduzione di nuovi diritti degli interessati (limitazione, oblio, portabilità)** **Art. (15-22)**
Corretta regolamentazione dei ruoli con contratti ad hoc	**Nuovo concetto di responsabile e regolamentazione dei subfornitori** **Art. (28)**	**Privacy by Design / Privacy by Default** **Art. (25)**
Tenuta dei Registri delle Attività di Trattamento **Art. (30)**	**Nuove misure di sicurezza: pseudonimizzazione, anonimizzazione e cifratura** **Art. (32)**	**Comunicazione delle violazioni all'Autorità e agli interessati** **Art. (33, 34)**
Valutazione d'impatto sulla protezione dei dati **Art. (35)**	**Introduzione della figura del DPO** **Art. (37, 38, 39)**	**Certificazione e codici di condotta** **Art. (42, 43)**

PRINCIPI (Qualità - art. 5)

I dati devono essere:

a) trattati in modo **lecito**, **equo** e **trasparente** nei confronti dell'interessato;

b) raccolti per **finalità determinate**, **esplicite** e **legittime**, e successivamente trattati in modo non incompatibile con tali finalità;

c) «**adeguati**, **pertinenti** e **limitati**» a quanto necessario rispetto alle finalità per le quali sono trattati ("**minimizzazione dei dati**");

d) «**esatti** e **aggiornati**» (i dati inesatti devono essere rettificati o cancellati);

e) conservati in una forma che consenta l'identificazione dell'interessato per un **arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati: "**limitazione della conservazione**");

f) trattati in modo da garantire un'**adeguata sicurezza** dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("**integrità e riservatezza**") → **SICUREZZA come presupposto del trattamento**

PRINCIPI (Liceità - art. 6)

Il trattamento dei dati personali 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 [*NO consenso per gli Enti pubblici*];
f) il trattamento è 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 (in particolare se l'interessato è un minore).

BASI GIURIDICHE:

- **Base giuridica del trattamento (art. 6)**
- **Base giuridica ex art. 9**

Basi giuridiche ex art. 9

- Consenso dell'interessato
- Esercizio obblighi in materia di diritto del lavoro
- Esercizio obblighi in materia di protezione sociale
- Tutela interesse vitale dell'Interessato
- Trattamento ex art. 9 lett. d) GDPR
- Dati personali resi pubblici dall'Interessato
- Trattamento in sede giudiziaria
- Trattamento per interesse pubblico rilevante
- Finalità di medicina
- Interesse pubblico per sanità pubblica
- Archiviazione nel pubblico interesse
- Ricerca storica o statistica
- Esistenza del segreto professionale

INFORMATIVA – ART. 13
(quando i dati sono raccolti presso l'interessato)

Il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a)l'identità e le coordinate di contatto del titolare del trattamento e del suo eventuale rappresentante

b) le coordinate di contatto dell'eventuale responsabile della protezione dei dati (DPO);

c)la base giuridica e le finalità del trattamento cui i dati personali sono destinati;

d)i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e)gli eventuali destinatari o le categorie di destinatari dei dati personali;

f)ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

Qualora il titolare del trattamento intenda trattare ulteriormente i dati per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale finalità diversa e tutte le informazioni pertinenti di cui al paragrafo 2.

INFORMATIVA – ART. 13
(quando i dati sono raccolti presso l'interessato - paragrafo 2)

Nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo ad un'autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Adempimenti conseguenti ad una violazione di dati personali (Artt. 33-34 Regolamento UE)

- Notificazione della violazione all'autorità di controllo senza ritardo;

- Entro 72 ore dalla conoscenza (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

- Successivamente le 72 ore solo con giustificazione motivata;

- Obbligo di allerta da parte del Responsabile del trattamento;

- Comunicazione della violazione all'interessato;

- Il Titolare del trattamento documenta qualsiasi violazione dei dati personali (circostanze, conseguenze e provvedimenti adottati per porvi rimedio).

Tipo di violazione

- Lettura (presumibilmente i dati non sono stati copiati)
- Copia (i dati sono ancora presenti sui sistemi del titolare)
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- Altro …..

DATA BREACH

MENU

la Repubblica.it

ACCEDI

HOME MACROECONOMIA FINANZA LAVORO DIRITTI E CONSUMI AFFARI&FINANZA OSSERVA ITALIA GLOSSARIO LISTINO PORTAFOGLIO

Caos Spesometro, l'Agenzia concede il rinvio. E il sito tornerà in funzione domani

Ma per i commercialisti il tempo resta poco. Il servizio per l'invio telematico delle fatture era stato bloccato nel fine settimana dopo che era emersa un'importante falla sulla privacy dei contribuenti. La scadenza prevista per il 28 settembre slitterà al 5 ottobre

I soggetti, i compiti e le responsabilità

I RUOLI e LE RESPONSABILITA':

Viene ridisegnato l'organigramma privacy, con l'introduzione di nuove figure soggettive e l'attribuzione di nuovi compiti e responsabilità:

- **Titolare del trattamento** (*data controller*);
- **Contitolare** (*joint controller*);
- **Responsabile del trattamento** (*data processor*);
- **Sub-responsabile** (*subprocessor*);
- **Responsabile della protezione dei dati** o *Data Protection Officer* (DPO).

Il Regolamento Europeo: il Titolare

Tenuto conto della **natura**, del **campo di applicazione**, del **contesto** e delle **finalità del trattamento**, nonché dei **rischi** di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

IL CONTITOLARE

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali, essi sono **contitolari del trattamento**. Essi determinano in modo trasparente, mediante un **accordo interno**, le rispettive responsabilità in merito:

- all'osservanza degli obblighi derivanti dal regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato,
- alle rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14.

Tale accordo può designare un punto di contatto per gli interessati.

L'interessato può esercitare i propri diritti **nei confronti di e contro** ciascun titolare del trattamento.

L'accordo riflette adeguatamente i rispettivi ed effettivi ruoli dei contitolari del trattamento e i loro rapporti con gli interessati, e il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Il Regolamento Europeo: il Responsabile

Art. 28, paragrafo 3

L'esecuzione dei trattamenti su commissione è disciplinata da un **contratto** o da **altro atto giuridico** 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 la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Diventa un negozio giuridico sinallagmatico tra titolare del trattamento e responsabile privacy, che genera obbligazioni e responsabilità reciproche in materia di protezione dei dati personali

Ai sensi di quanto previsto nel Regolamento UE si pone, quindi, in primo piano il problema della **corretta contrattualizzazione dei rapporti** tra i soggetti titolari/contitolari/responsabili/sub-responsabili coinvolti i quali, a seconda dello specifico trattamento effettuato, concorreranno a vario titolo nella gestione delle attività di trattamento (in quanto insieme o separatamente possono determinano le finalità, le condizioni e i mezzi del trattamento).

La mancata contrattualizzazione o la mancanza di chiarezza nella contrattualizzazione (*anche in materia di adozione di specifiche misure di sicurezza*), possono implicare una responsabilità.

E i vecchi Incaricati del d.lgs. 196/2003?

Trattamento sotto l'autorità del titolare del trattamento e del responsabile del trattamento (art. 29 del nuovo Regolamento)

Il responsabile del trattamento, o **chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento**, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

ATTENZIONE: i titolari e i responsabili del trattamento hanno l'obbligo di formazione e istruzione nei confronti dei soggetti (persone fisiche) che trattano dati personali (denominati anche quali "*le persone autorizzate al trattamento dei dati personali*" ovvero "*personale che partecipa ai trattamenti*")

Il c.d. Data Protection Officer (Responsabile della Protezione dei Dati)

Il Regolamento Europeo: il DPO

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un **responsabile della protezione dei dati** quando:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala (=*profilazione*);
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10 (=*dati sensibili e/o giudiziari*).

Esempi di attività principale

1) un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche: l'attività principale consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali → l'impresa deve nominare un RPD

2) l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute (es. informazioni contenute nella cartella sanitaria di un paziente): il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale → gli ospedali devono nominare un RPD

3) organismi che svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico: sono funzioni di supporto necessarie all'attività principale o dell'oggetto principale dell'organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali → non deve essere nominato un RDP

Il «DPO» deve essere facilmente raggiungibile da ciascuno stabilimento in quanto è il punto di contatto:

- per gli interessati ("*Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento*");
- per l'autorità di controllo (deve "*fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione*");
- per i soggetti interni all'azienda o all'ente (visto che uno dei compiti del DPO consiste nell'*informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento*).

Nuove Faq sul Responsabile della Protezione dei Dati in ambito privato

Sono tenuti alla nomina del DPO:

- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie e società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti e istituti di vigilanza;
- partiti e movimenti politici;
- sindacati, caf e patronati;
- società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas);
- imprese di somministrazione di lavoro e ricerca del personale;
- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione;
- società di call center;
- società che forniscono servizi informatici.

Il DPO è designato in funzione delle sue **qualità professionali** e della **capacità di adempiere ai compiti** di cui all'articolo 39:

- conoscenza specialistica della **normativa**;

- conoscenza delle **pratiche** in materia di protezione dei dati;

- può essere un **membro del personale** del titolare del trattamento o del responsabile del trattamento oppure adempiere ai suoi compiti in base a un **contratto di servizi**;

- il titolare del trattamento o il responsabile del trattamento **pubblica le coordinate di contatto** del responsabile della protezione dei dati e le **comunica all'autorità di controllo**;

- deve essere prontamente e adeguatamente **coinvolto** in tutte le questioni riguardanti la protezione dei dati personali;

- titolare del trattamento e responsabili forniscono al DPO le **risorse necessarie** per adempiere alle sue funzioni (di cui all'articolo 39), nonché l'accesso ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

I **quattro livelli di competenze e capacità** del DPO:

- Livello di esperienza

(commisurato alla sensibilità, complessità e quantità di dati trattati dal titolare/responsabile del trattamento: a maggiore complessità e quantità di dati scaturisce un più elevato livello di competenza e supporto)

- Qualità professionali

(conoscenza approfondita del Regolamento, esperienza sulle leggi in materia di protezione dei dati a livello nazionale ed europeo, conoscenza del settore e dell'organizzazione del titolare del trattamento, dei sistemi informatici/informativi e delle esigenze di sicurezza e di protezione dei dati; per le PA occorre anche una buona conoscenza delle regole e delle procedure dell'organizzazione amministrativa)

- Capacità di svolgimento dei compiti

(Integrità e alta etica professionale, preoccupazione circa il rispetto della conformità al Regolamento, promozione di una cultura della protezione dei dati all'interno dell'organizzazione)

- DPO sulla base di un contratto di servizio

(possibilità di esternalizzare tale funzione mediante un contratto di servizi ad una organizzazione esterna: persona giuridica/ente collettivo; i compiti potranno essere eseguiti non solo da un singolo professionista della privacy, ma da una sorta team esterno che fornisce il servizio di DPO)

Il Regolamento Europeo: il DPO

• Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento;

• Adempie alle sue funzioni in piena **indipendenza** e non riceve alcuna istruzione per quanto riguarda il loro esercizio;

• **Non è rimosso** o **penalizzato** dal titolare del trattamento o dal responsabile del trattamento **per l'adempimento dei propri compiti**;

• **Riferisce** direttamente ai **massimi superiori gerarchici** del titolare del trattamento o del responsabile del trattamento;

• E' tenuto al **segreto** o alla **riservatezza** in merito all'adempimento dei propri compiti;

• Può svolgere altri compiti e funzioni, purché non diano adito a un **conflitto di interessi**.

Compiti e Funzioni che possono implicare conflitti di interessi

Per tali motivi non può essere un DPO in quanto possono sussistere situazioni di conflitto con riguardo a ruoli manageriali di vertice:

- l'amministratore delegato,
- il responsabile operativo,
- il responsabile finanziario,
- il responsabile sanitario,
- la direzione marketing,
- la direzione risorse umane,
- il responsabile IT.

Compiti del responsabile della protezione dei dati

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento -nonché i dipendenti che eseguono il trattamento- in merito agli **obblighi** derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo (*audit*);

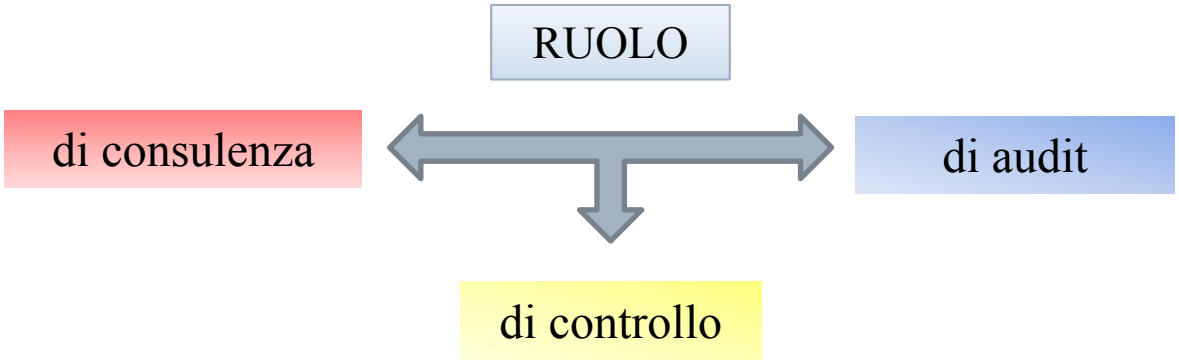
f) **fornire**, se richiesto, un **parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento** ai sensi dell'articolo 33;

g) **cooperare con l'autorità di controllo**;

h) fungere da **punto di contatto per l'autorità di controllo** per questioni connesse al trattamento di dati personali, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni su qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del medesimo.

Compiti del responsabile della protezione dei dati (DPO=facilitatore della *compliance*)



Secondo le Linee Guida del WP 29, fanno parte di questi compiti di controllo svolti dal DPO, in particolare,
- la raccolta di informazioni per individuare i trattamenti svolti,
- l'analisi e la verifica dei trattamenti in termini di loro conformità, e
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Fuori dagli obblighi, la nomina del DPO è comunque una scelta saggia e vincente!

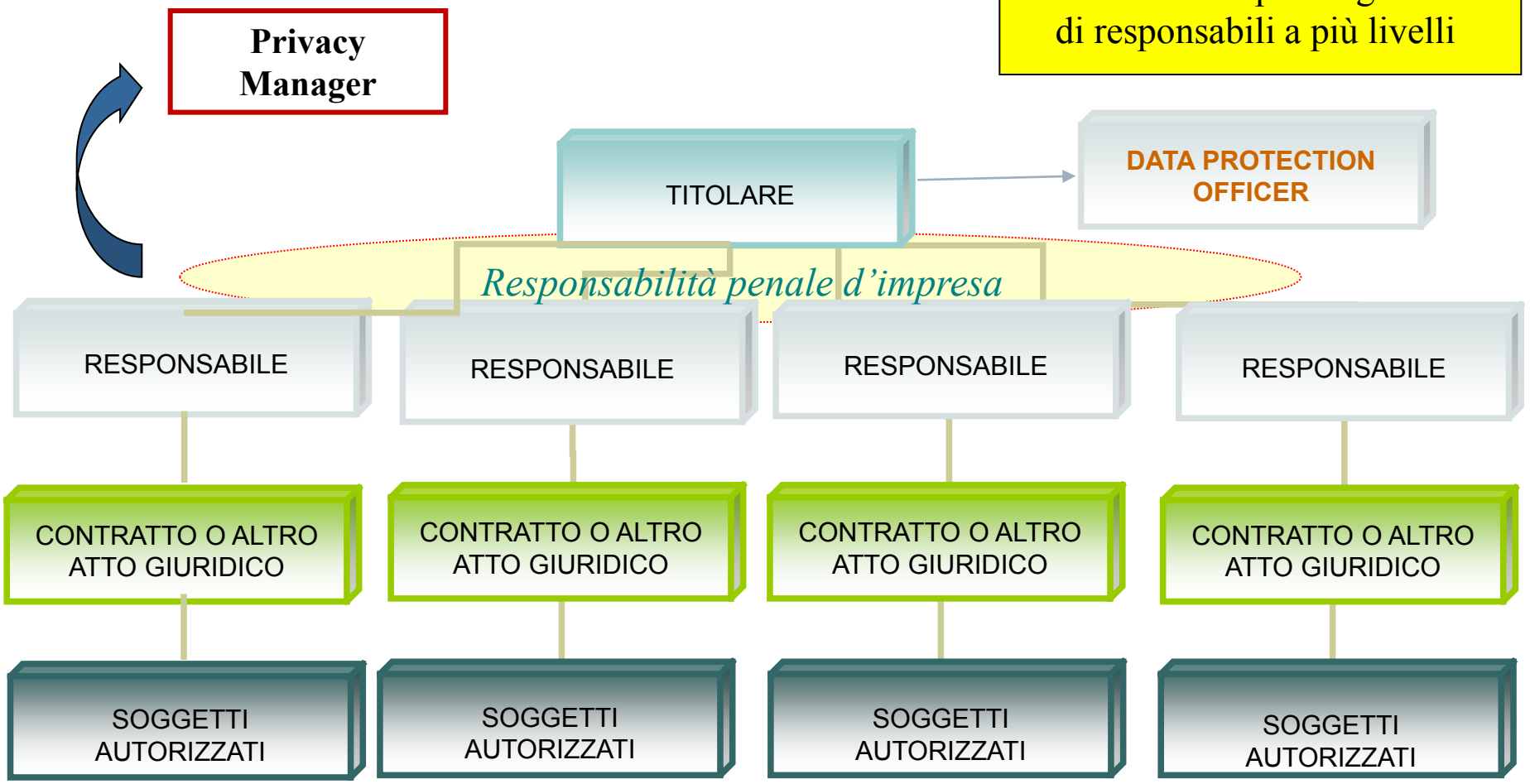
Coinvolgimento del DPO in tutte le questioni riguardanti la protezione dei dati personali

Occorrerà garantire:
- che il DPO sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del DPO ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il DPO deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del DPO riceva sempre la dovuta considerazione. In caso di disaccordi, il WP29 raccomanda (quale buona prassi) di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal DPO;
- che il DPO sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

N.B.: sono opportune linee-guida o regolamenti interni in materia di protezione dei dati che indichino i casi di consultazione obbligatoria del DPO

L'organizzazione

In strutture complesse gerarchia di responsabili a più livelli



Il DPO non può essere personalmente responsabile in caso di mancato rispetto degli obblighi e adempimenti previsti dal GDPR in capo al titolare o al responsabile del trattamento

Sicurezza del trattamento (Art. 32)

1. Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento **mettono in atto misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso:

a) la **pseudonimizzazione** e la **cifratura** dei dati personali;
(utile in caso di data breach)

b) la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi che trattano i dati personali;
(capacità di adattamento a condizione d'uso e resistenza a situazioni avverse per garantire disponibilità dei servizi erogati)

c) la capacità di **ripristinare** tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
(procedure di DR e incident response)

d) una procedura per **testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.
(come per la ISO 27001 o per il D.Lgs. 231/2001)

Il Registro delle attività di trattamento

Registro delle attività di trattamento

Ogni **TITOLARE del trattamento** e il suo eventuale rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Il registro contiene le seguenti informazioni:

- il nome e le coordinate di contatto del titolare del trattamento e di ogni contitolare del trattamento, del rappresentante del titolare del trattamento e dell'eventuale responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi;
- trasferimenti di dati verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative.

Registro delle attività di trattamento

Ogni **RESPONSABILE del trattamento** e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività di trattamento dei dati personali svolte per conto di un TITOLARE del trattamento, contenente:

- il nome e coordinate di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e dell'eventuale responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- i trasferimenti di dati verso un paese terzo o un'organizzazione internazionale;
- una descrizione generale delle misure di sicurezza tecniche ed organizzative.

Esenzioni dalla tenuta del «Registro delle attività di trattamento»

Tali obblighi non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9 o il trattamento di dati relativi a condanne penali e a reati di cui all'articolo 10

I registri sono tenuti in forma scritta, anche in formato elettronico

Nella sezione dedicata al registro dei trattamenti il Garante sottolinea i seguenti concetti relativi al registro:

- ✓ **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico;
- ✓ **indispensabile per ogni valutazione e analisi del rischio**.

Inoltre

- ✓ La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**.
- ✓ Per tale motivo, ***"si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro".***
- ✓ Nello specifico, si richiama l'attenzione sulla sostanziale **coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art. 30 regolamento.**

Perché è importante il Registro delle Attività di Trattamento

- rientra a pieno titolo tra i nuovi **obblighi di compliance** a cui sono tenuti i titolari e i responsabili del trattamento (quale misura organizzativa adeguata ed efficace);
- aiuta titolari e i responsabili del trattamento a realizzare quel nuovo principio dell'**accountability** (responsabilizzazione) di cui è permeato l'intero Regolamento europeo;
- viene considerato dai Garanti europei (WP29) un **prerequisito per la conformità al GDPR** e misura di **responsabilizzazione efficace**.

Come gestire le nuove tematiche e le opportunità per i commercialisti con particolare riguardo al Registro

- Individuare **nuove aree di business: ad esempio**, la valutazione della necessità o meno di designare un DPO
- La tenuta del registro dei trattamenti
- La redazione delle clausole contrattuali con gli outsourcers ex art. 28 GDPR
- La redazione delle clausole contrattuali con gli outsourcers ex art. 28 GDPR
- Lo svolgimento della valutazione di impatto (DPIA)
- **Informare la clientela e supportarla** nella gestione delle nuove tematiche introdotte dal GDPR
- Valutare l'opportunità di **creazione di «desk» di professionisti dedicati**
- Assumere, se in possesso dei requisiti, il ruolo di **DPO esterno**

Sanzioni (nel Regolamento)

Condizioni generali per irrogare sanzioni amministrative pecuniarie

Ogni autorità di controllo garantisce che le sanzioni amministrative pecuniarie irrogate ai sensi del presente articolo in relazione alle violazioni del presente regolamento siano in ogni singolo caso **effettive**, **proporzionate** e **dissuasive.**

Le sanzioni amministrative pecuniarie sono irrogate, in funzione delle circostanze di ogni singolo caso.

Al momento di decidere se irrogare una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

- la natura, la gravità e la durata della violazione in considerazione della natura, del campo di applicazione o della finalità del trattamento in questione, nonché del numero di interessati lesi dal danno e del livello del danno da essi subito;
- il carattere doloso o colposo della violazione;
- le misure prese dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- il grado di responsabilità del titolare del trattamento o del responsabile del trattamento, considerate le misure tecniche e organizzative da essi messe in atto;
- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

- le categorie di dati personali interessate dalla violazione;
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- qualora siano stati precedentemente imposti provvedimenti (avvertimenti, moniti, ingiunzioni varie ovvero «poteri correttivi» dell'Autorità di controllo ai sensi dell'art. 53), nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- l'adesione ai codici di condotta o ai meccanismi di certificazione;
- eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i vantaggi finanziari conseguiti o le perdite evitate (direttamente o indirettamente) quale conseguenza della violazione.

SANZIONI

La violazione delle disposizioni comporta sanzioni amministrative pecuniarie:

- **fino a 10 milioni di EURO, o per le imprese, fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente;
- **fino a 20 milioni di EURO, o per le imprese, fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente.

La mancata osservanza di un ordine da parte dell'autorità di controllo è soggetta a sanzioni amministrative pecuniarie **fino a 20 milioni di EURO, o per le imprese, fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore.

***Ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere irrogate sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro*.**

GRAZIE PER L'ATTENZIONE!!!

Avv. Graziano Garrisi
Privacy consultant – Responsabile della Protezione dei dati
Data Protection Auditor
grazianogarrisi@gmail.com
grazianogarrisi@pec.it