Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

OdV e Privacy

Paola Zambon
Dottore Commercialista

i Webinar
by Directio

WEBINAR > **20 ANNI DI "231": ASPETTI CONSOLIDATI E POSSIBILE EVOLUZIONE NORMATIVA, REFRESH DEI MODELLI ORGANIZZATIVI A FRONTE DELLE NUOVE PREVISIONI DI REATI PRESUPPOSTO**

A cura dell'ODCEC di Torino

21/09/2020

Il «Regolamento generale sulla protezione dei dati»

- GDPR, «General Data Protection Regulation» o Regolamento UE 2016/679
- Il testo, pubblicato nella GUCE il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno ha iniziato ad avere efficacia il 25 maggio 2018.
- Dopo due anni di piena applicazione, a seguito dell'epidemia Covid, spesso si è trattato di limitare i diritti che il GDPR intende proteggere…

Protezione di:
diritti e le libertà fondamentali delle **persone fisiche,** in particolare il diritto alla protezione dei dati personali

IMPLICA in tempi di covid

FIDUCIA delle persone interessate affinché i loro diritti e le loro libertà siano rispettati

ADEGUATE MISURE nei mezzi tecnologici scelti

TRASPARENZA sul trattamento

TAVOLO CONGIUNTO GDPR ORDINI PROFESSIONALI DI TORINO

Gli Ordini dei **Dottori Commercialisti** ed Esperti Contabili, degli **Avvocati** e degli **Ingegneri** di Torino,

hanno lavorato assieme per affrontare al meglio il cammino verso il GDPR

Il tavolo si è espresso anche in tema di qualificazione soggettiva dell'Odv ai fini privacy a giugno 2020

Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

ORDINE DEGLI AVVOCATI DI TORINO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO

Un supporto per le nostre Categorie

- Evidenziare l'importanza della norma sensibilizzando in particolare sugli effetti della «responsabilizzazione»
- Informare e formare i Professionisti nei propri studi professionali
- Offrire spunti utili per impostare i propri lavori e suggerimenti applicativi
- Invitare i colleghi che hanno maturato esperienza in materia di protezione dei dati personali a proseguire nella loro attività dedicando una particolare attenzione all'auto-formazione
- Essere di riferimento verso le Autorità competenti

Il Tavolo vi invita al prossimo webinar
20/11/2020 in tema di privacy e di e-commerce
invito prossimamente pubblicato su
www.ictdott.com
e siti dei nostri Ordini Professionali

General Data Protection Regulation

DEFINIZIONI

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

Titolare del trattamento

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento

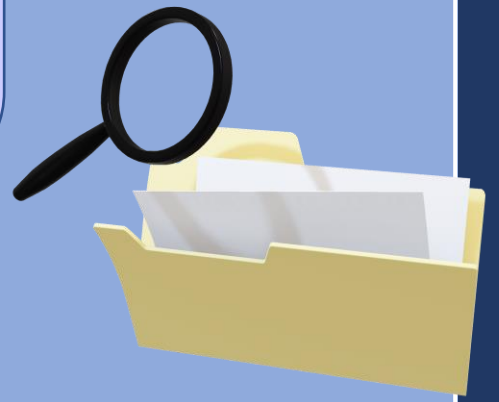
Contitolare

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che tratta dati personali per conto del titolare del trattamento**

Responsabile del trattamento

Persona fisica che svolge specifici compiti e funzioni connessi al trattamento di dati personali, espressamente designata, **che opera sotto l'autorità del Titolare o del Responsabile, sotto la responsabilità e nell'ambito dell'assetto organizzativo di questi ultimi**

Designati/Autorizzati



Accountability e «Privacy Governance»

Art. 24) GDPR: il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per

- garantire ed
- essere in grado di dimostrare

che il trattamento è effettuato conformemente al GDPR

Privacy Governance: esempi

- Privacy by design e by default
- Organizzazione interna privacy
- Registro attività del trattamento
- Policy, procedure e contratti
- Gestione del rischio e documentazione su decisioni prese
- Misure adeguate tecniche ed organizzative
- Procedure data breach
- Valutazione d'impatto
- Codici di condotta e schemi di certificazione

OdV e Privacy

Ruolo Odv - ex D.Lgs. 231/01 – art. 6 c. 1 lett. b)

- Il compito di **vigilare sul funzionamento e l'osservanza dei modelli organizzativi 231** e di curare il loro aggiornamento è «affidato ad un organismo dell'ente **dotato di autonomi poteri di iniziativa e di controllo**».

Dati personali trattati nei:

- Flussi informativi periodici
- Flussi informativi ad hoc
- Segnalazioni di condotte illecite o altre violazioni

Garante: Il modello deve «prevedere obblighi di informazione nei confronti dell'OdV (art. 6, comma 2, lett. d), d.lgs. n. 231/2001), con flussi di informazioni (periodici e ad hoc) che avvengono attraverso specifici processi di comunicazione aziendale al fine di conoscere e gestire eventuali situazioni di rischio.
Analoga attività di informazione sarà svolta dall'OdV nei confronti del vertice in merito al funzionamento e all'aggiornamento del modello o in presenza di eventuali criticità rilevate nell'ambito dell'attività di vigilanza. L'OdV può ricevere anche segnalazioni di condotte illecite rilevanti o di violazioni del modello così come previsto» dalla norma.

Odv: alcune riflessioni

Parere sulla qualificazione soggettiva ai fini privacy degli O.d.V. del 12/05/2020 - In risposta al quesito posto dall'Associazione dei Componenti degli Organismi di Vigilanza (AODV)

RUOLO EFFETTIVO?

- Consulente sull'efficacia del modello organizzativo
- Segnalatore di criticità riscontrate nella propria attività di vigilanza
- DPO
- Alcune analogie anche in : organi di controllo – società di revisione - Medico del lavoro (indipendenza) - Professionista

art. 4, n. 7 GDPR – Titolare:
"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".

art. 4, n. 8 GDPR – Responsabile:
"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del titolare del trattamento**".

Fa parte dell'azienda dunque l'ODV non è né titolare né responsabile. **I suoi membri sono meri autorizzati**

MEZZI/STRUMENTI

Come l'Odv gestisce la documentazione cartacea e digitale? Non dovrebbe farlo in modo indipendente dall'azienda?

- **La continuità d'azione è garantita** in modo che l'operatività dei membri non condizionino l'obiettività dei loro giudizi?

INDIPENDENZA. AUTONOMIA. PROFESSIONALITA'

I membri dell'Odv dovrebbero essere indipendenti, autonomi e professionalmente preparati rispetto agli esponenti degli organi sociali

ACCESSO AI DATI AZIENDALI

Se l'Odv è come fosse un lavoratore aziendale allora può essere limitato nell'accesso ai dati aziendali? La propria discrezione di indagine è garantita? Come può garantire la tracciabilità del proprio lavoro? Necessario definire accordi

EFFICACIA CAUSALE DELL'ODV

La violazione in tema di trattamento di dati personali eventuale effettuata dall'Odv può essere sempre imputabile all'ente anche nel whistleblowing?

Odv al centro di esegesi copiose e spesso discordanti

- Spesso sono professionisti esterni (che si avvalgono anche di propri tirocinanti) e che conservano le carte di lavoro nei propri studi professionali
- L'ente definisce il modello ma poi fornisce realisticamente procedure adeguate per «comandare» e controllare tali informazioni negli uffici dei singoli professionisti?
- I regolamenti dovrebbero essere scritti dall'Odv….
- La maggiore parte dei regolamenti rimandano a generiche clausole di riservatezza…
- In caso di segnalazioni la conservazione di tale documentazione è di consueto effettuata dall'Odv con strumenti da lui scelti…

Focus

Organi di amministrazione, direzione o controllo di società controllate e partecipate

Nel caso di specie, per persone politicamente esposte si intendono l'amministratore unico, i componenti del consiglio di amministrazione, il direttore generale, i componenti del collegio sindacale e i componenti del consiglio di sorveglianza. Non vi rientrano i componenti dell'organismo di vigilanza *ex* D.Lgs. 231/2001 e il revisore esterno, in quanto non costituiscono "organi" della società.

LINEE GUIDA PER LA VALUTAZIONE DEL RISCHIO, ADEGUATA VERIFICA DELLA CLIENTELA, CONSERVAZIONE DEI DOCUMENTI, DEI DATI E DELLE INFORMAZIONI AI SENSI DEL D.LGS. 231/2007 – Cndcec – in merito alle definizione di persone politicamente esposte

Il fatto di dover riportare direttamente all'organo di amministrazione pone l'Odv in posizione verticistica

Sintesi mie interpretazioni presentate al Cndcec per il Commercialista (gennaio 2019) ora confermate dal Comitato Europeo per la protezione dati personali nel recente documento in consultazione pubblica

art. 4, n. 7 GDPR – **Titolare:**

“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”.

Nel caso in cui il Commercialista riceva un mandato per prestazioni o attività, consulenze o pareri senza alcun tipo di istruzione da parte del cliente, sarà autonomo titolare del trattamento poiché «processa» autonomamente le modalità di trattamento.

Il Commercialista che tratta dati personali del cliente in attuazione di norme obbligatorie (es. s.o.s. antiriciclaggio) è parimenti titolare del trattamento (non agisce né con il consenso del cliente e né con il consenso di terzi ma per obbligo professionale richiesto da una norma). Stesso ruolo di titolare, a mio avviso, viene ricoperto per analoghi motivi il revisore (esterno) ed il curatore fallimentare.

Viceversa quando riceva istruzioni (es. come contabilizzare una posta, cosa indicare nella relazione sulla gestione, come «orientare» la gestione di una problematica aziendale, come considerare le spese sostenute, ecc.) allora il Commercialista potrà essere Responsabile del Trattamento (ex art. 28 GDPR).

Considerazioni su Odv in tema di GDPR

Alcune considerazioni	Risposte analizzate per l'ODV
Chi decide sulla raccolta dei dati personali	L'ODV nell'ambito del mandato che svolge decide quali dati personali selezionare e verificare all'interno del modello impostato dall'organo di amministrazione (Garante asserisce che i loro compiti non sono determinati dall'Odv, ma dall'organo dirigente dell'ente (che, nell'ambito del modello di gestione e organizzazione, ne definisce gli aspetti relativi al funzionamento, l'attribuzione delle risorse, i mezzi e le misure di sicurezza) nonché dalla legge)
la base di liceità per farlo	L'ODV ha una base di liceità contrattuale con l'ente che gli ha chiesto la vigilanza (tramite nomina). Garante riconosce la responsabilità contrattuale
quali tipi di dati personali tratta	L'ODV raccoglie tutti i dati personali utili per svolgere il proprio compito (anche dati particolari)
Natura/scopo del trattamento	L'ODV raccoglie tutti i dati personali utili per svolgere il compito di vigilare sul funzionamento e l'osservanza del modello organizzativo (Garante asserisce eventuali omessi controlli sull'osservanza dei modelli predisposti dall'ente non ricadono sull'OdV ma sull'ente stesso)
Categorie di persone	Tipicamente dipendenti, clienti e fornitori dell'ente
Comunicazione di dati a terzi	Genericamente no se non in alcuni casi all'Autorità
Descrizione dello scopo	Trattamento per scopo vigilanza sul mod. org. az.
Chi risponde in caso di richiesta di esercizio dei diritti	Diritto di accesso potrebbe essere limitato dall'ente? Se si dovrebbe essere chiarito in ogni caso Nel whistleblowing?
per quanto tempo conservare i dati o se apportare modifiche non ordinarie ai dati.	Probabilmente 10 anni

Se si prende una qualsiasi di queste decisioni determinando gli scopi e i mezzi del trattamento, si potrebbe essere considerati responsabili nella casistica del whistleblowing?

COMPITI SUL MODELLO E REGOLAMENTO ODV: DIFFERENZE IMPORTANTI ANCHE PER DEFINIRE IL RUOLO DELL'ODV AI FINI GDPR

Il Garante asserisce che all'Odv debbano essere **assegnati i compiti** «dall'organo dirigente dell'ente che, **nell'ambito del modello di gestione e organizzazione**, ne definisce gli aspetti relativi al funzionamento, l'attribuzione delle risorse, i mezzi e le misure di sicurezza».

Confindustria, **Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo**, 2014, Cap. IV, par. 2.2, pag. 61

Confindustria suggerisce che "**l'OdV formuli un regolamento delle proprie attività** (determinazione delle cadenze temporali dei controlli, individuazione dei criteri e delle procedure di analisi, ecc.).
Non è, invece, consigliabile che tale regolamento sia redatto e approvato da organi societari diversi dall'OdV in quanto ciò potrebbe metterne in dubbio l'indipendenza"

Nel Regolamento l'ODV può esprimere la propria autonomia e indipendenza.

Le segnalazioni pervenute all'Odv, ad esempio, si ritiene che dovrebbero essere trattate nel Regolamento così come l'estensione ai propri collaboratori del segreto professionale, conflitto di interessi anche nel caso di violazioni GDPR, interventi previsti in gruppo o nel singolo componente Odv, ecc.

Quando si deve nominare un responsabile del trattamento?

Per poter agire come «responsabile del trattamento» occorrono due requisiti preliminari:

1) essere una persona giuridicamente distinta dal titolare del trattamento e
2) trattare dati personali per conto di quest'ultimo (con compiti limitati e precisati oppure con un margine di discrezionalità sul modo di servire gli interessi del titolare, individuando i mezzi tecnici ed organizzativi adeguati).

(parere 01/2010 sui concetti di «controller" e «processor» ex WP *art. 29 recente posizione del Comitato Europeo per la protezione dati personali)*

Appare evidente che dal momento in cui il titolare del trattamento decide di «dare in outsourcing» un trattamento di dati personali qualunque, la persona giuridicamente distinta da sé stesso possa essere considerata come minimo un responsabile esterno.

(L'art. 28 GDPR prevede che la nomina avvenga per iscritto)

Ruolo Odv in relazione alle segnalazioni effettuate nell'ambito della normativa di *whistleblowing* (art. 6, comma 2-*bis*, 2-ter, 2-*quater*, d.lgs. n. 231/2001)

- **Il Garante non si è pronunciato sul ruolo dell'Odv nel delicato ruolo previsto dal whistleblowing** «il d.lgs n. 231/2001 non attribuisce necessariamente all'OdV la gestione delle segnalazioni in questione, ma rimette alla discrezionalità dell'ente la scelta di individuare in un soggetto diverso il destinatario di tali segnalazioni che avrà il compito di istruirle e adottare ogni conseguente provvedimento»
- **E' lecito pensare però che l'Odv debba essere coinvolto nella segnalazione** (almeno per quanto riguarda gli illeciti tra quelli previsti da Modello 231, da parte di esponenti aziendali nell'interesse o a vantaggio della società);
- Ambiti diversi se ente è privato o pubblico (con canali non solo per i dipendenti ma anche per gli esterni nel secondo caso)
- In ogni caso sarebbe utile garantire la possibilità che le persone possano riferire direttamente all'odv sui comportamenti criminosi eventualmente riscontrati! Dunque la raccolta di dati personali anche particolarmente «delicati» dovrebbe essere mantenuta riservata e sotto segreto professionale con canali informatici adeguati

Odv e Whistleblowing - GDPR

Fattispecie inquadrabile con il responsabile del trattamento?

Odv come destinatario autonomo di denunce

Odv come mero conoscitore del flusso informativo «whisteblowing»

Fattispecie inquadrabile come autorizzato al trattamento?

- Per tutela l'integrità dell'ente
- Per tutelare il segnalante
- Nel caso di società a partecipazione pubblica il segnalante oltre al dipendente potrebbe essere il collaboratore di fornitori di servizi dunque occorre prevedere un canale differenziato

Odv ed indipendenza in lettura GDPR

- l'Odv nell'esecuzione dei compiti attribuitigli dall'art. 6 D.Lgs. 231/01 e dall'ente, **non deve ricevere istruzioni sull'approccio da seguire** (es. quali siano i metodi migliori per condurre gli accertamenti sull'efficacia del modello, sulla sua osservanza o per curare il relativo aggiornamento).
- L'assenza di conflitti di interessi è strettamente connessa al concetto di indipendenza: **occorre verificare se sussistano casistiche tali nel trattamento di dati personali che possano influire su tale indipendenza**.

Funzioni dell'Odv desunte dall'art. 6 c. 1 lett. b) D.Lgs. 231/01:
(L'Organismo di vigilanza ha)
«il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente ***dotato di autonomi poteri di iniziativa e di controllo****»*

La condotta dell'Odv nel whistleblowing ai fini GDPR: alcune utili interpretazioni in attesa di chiarimenti

1. Se si assume che il singolo membro dell'Odv possa «conservare» con criteri e metodi diversi le proprie carte di lavoro qualora uno dei membri subisse un data breach, non si ritiene che ai fini di evitare quel rischio si possa estendere la responsabilità del singolo componente all'intero Odv
2. Se l'Odv fosse considerato responsabile del trattamento in caso di data breach sul whistleblowing la propria responsabilità dovrebbe essere comunque limitata a quanto previsto negli accordi contrattuali con l'ente
3. Dal momento in cui ogni singolo membro Odv di fatto potrebbe assumere un comportamento scorretto in tema di trattamento di dati personali, riterremo utile riflettere anche sui singoli ruoli degli stessi in caso di whistleblowing (es. sarebbe possibile veicolare maggiori responsabilità al Presidente Odv rispetto a quelle degli altri membri autorizzati attraverso il regolamento?)

Reati informatici e Covid: sempre alta l'attenzione!

Lo smart working ha favorito il lavoro da casa. Sono sorti diversi problemi:

1) I dipendenti potrebbero non pensare alla sicurezza informatica e potrebbero utilizzare devices propri con app sconosciute se le policy non fossero adeguate.
2) Sono sorti siti web e email in tema di Covid per fare «cascare» l'utente con la scusa di tematiche interessanti
3) Sono sorte truffe commerciali (mascherine, disinfettanti o vitamine «miracolose», false raccolte fondi, ecc.)
4) **Sono aumentati i casi di phishing** (soprattutto a danni di aree HR per email in cui per accedere a sondaggi interessanti sul come adeguarsi venivano richieste credenziali di Office ecc.)
5) Attacchi informatici anche contro Governi ed imprese segnalati e condannati nel Regno Unito

Report claims human error is major cause of UK breaches

Il 90% delle violazioni dei dati nel Regno Unito sono causate da errori umani (rapporto National Cyber Security Centre febbraio 2020)

UK condemns Chinese cyber attacks against governments and businesses

The UK has today joined international allies to call out malicious cyber activity carried out by China.

PUBLISHED
16 September 2020

Per chi desidera essere gratuitamente aggiornato su queste tematiche segnalo il gruppo «Data Protection's corner» in Linkedin

https://www.linkedin.com/groups/8617764

Gruppo in Linkedin

GDPR…

Si attendono inoltre approfondimenti da parte del Garante

È importante il continuo aggiornamento su queste tematiche

© Paola Zambon

paolazambon@taxlawplanet.net

TaxLawPlanet™

Vi Invito al Webinar gratuito con il Politecnico di Torino:
20 novembre 2020
prossimamente su
www.ictdott.com