Convegno Associazione ICT Dottori Commercialisti

LE NOSTRE RIFLESSIONI

TAVOLO CONGIUNTO «PROTEZIONE DEI DATI PERSONALI – GDPR» ORDINI PROFESSIONALI

COMMERCIALISTI, AVVOCATI ED INGEGNERI

ORDINI DI TORINO

PAOLA ZAMBON – DOTTORE COMMERCIALISTA - REFERENTE GDPR ORDINE COMMERCIALISTI

CLAUDIO STRATA – AVVOCATO – REFERENTE GDPR ORDINE AVVOCATI

PAOLO TRAVERSA - INGEGNERE - REFERENTE GDPR ORDINE INGEGNERI

Webex, 20/11/2019

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

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

Attività svolta dal Tavolo congiunto GDPR

PRIMA DELL'ENTRATA in piena applicazione del GDPR:

autunno 2017: incontri di studio e pianificazione eventi

19/02/2018: inviata circolare agli iscritti relativa alle novità contenute nel GDPR e check list per gli studi professionali

12/03/2018: convegno presso il Tribunale di Torino con la spiegazione dell'utilizzo della checklist ed altri suggerimenti operativi

DOPO L'ENTRATA in piena applicazione del GDPR:

14/06/2018: convegno presso il Tribunale di Torino dal titolo "GDPR e nuova normativa italiana: riflessi su professionisti e PMI".

23/11/2018: convegno Associazione ICT Dott.Com – Politecnico di Torino: nostre interpretazioni operative

24/05/2019: Convegno presso il Tribunale di Torino "Privacy: il GDPR un anno dopo"

22/11/2019: convegno Associazione ICT Dott.Com – Politecnico di Torino: nostre riflessioni

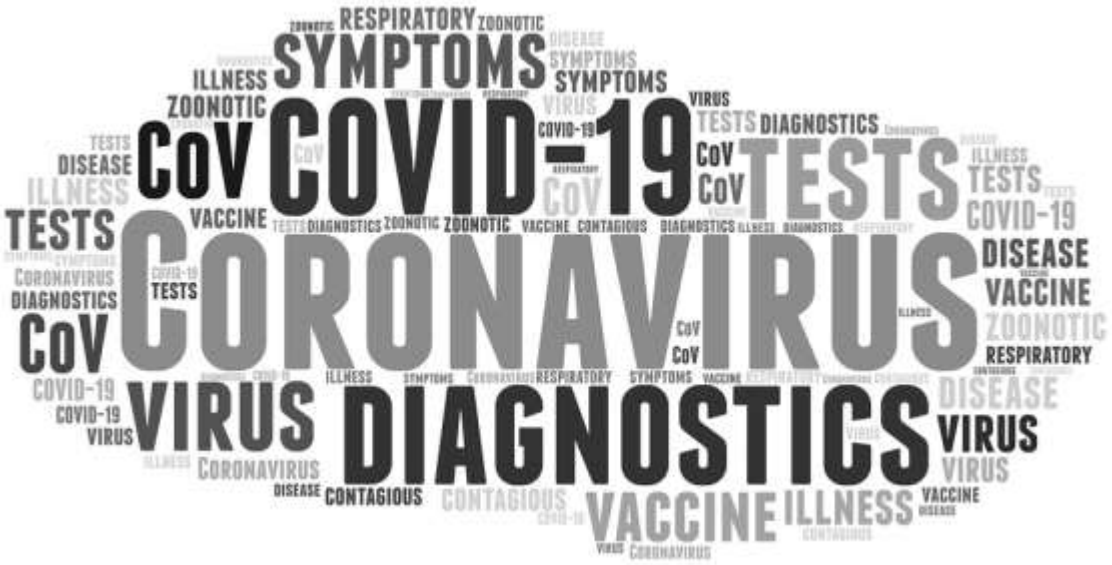
22/06/2020: convegno «ODV e privacy: aggiornamenti al tempo del COVID»

Evento online

Trattamenti «COVID» dei dati

Durante questi mesi ai sensi di DPCPM e ordinanze varie:

- Raccolta dati (nome e numero telefono) nei ristoranti/ parrucchieri/ palestre/ …
- Termoscanner
- Comunicazioni aziendali
- Dati in Smartworking



Problemi possibili

- Luogo del trattamento?
- Tempi di conservazione dei dati?
- Base legale del trattamento?
- Informative?!?!?
- Destinatari delle comunicazioni?
- Trattamenti di dati fuori dalle protezioni aziendali

Come comportarsi

Punto	Indicazioni Garante/ ordinanze nazionali o regionali/ suggerimenti	FAQ Garante Contesto lavorativo pubblico e privato
Tempi di conservazione dei dati	14 gg (30 gg Lazio) nelle ordinanze regionali	
Base legale del trattamento	Protocollo tra Governo e parti sociali del 14/3/20	2 e 8
Informative/ registro trattamenti	Aggiornare quelle esistenti	
Destinatari delle comunicazioni	Solo Autorità sanitarie (NO RLS e colleghi)	5 e 6
Registrazione automatica dati (Termoscanner e simili)	NO	10
Trattamenti dati in smartworking	Non cambiano le basi del trattamento. Si devono prendere maggiori precauzioni (DPIA da modificare??)	-

ASPETTI GIURIDICI E SANZIONATORI

***

Avv. Claudio STRATA

Il garante privacy e l'ODV

Un'efficace adozione del Modello di Organizzazione, Gestione e Controllo ex D.lgs. 231/2001, che permette alla società di andare esente da tale responsabilità, presuppone l'individuazione di un Organismo di Vigilanza, preposto a sorvegliarne l'attuazione.

L'art. 6 del D.lgs. 231/2001 enuncia il ruolo dell'OdV, che ha "*il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento*", in qualità di ente "*dotato di autonomi poteri di iniziativa e di controllo*".

Nello svolgimento della propria attività, dunque**, l'OdV tratta una moltitudine di dati personali, anche di carattere particolare (di cui agli artt. 9 e 10 G.D.P.R.), come notizie su eventuali illeciti commessi.**

Come esempi di trattamento possiamo citare:

- **Flussi informativi** in conformità agli obblighi di informazione nei confronti dell'OdV, deputato a vigilare sul funzionamento e l'osservanza dei modelli
- Risultati delle **attività di vigilanza e audit** effettuate
- **Segnalazione di fatti** che potrebbero configurarsi quali ipotesi di reato imputabili all'ente (c.d. whistleblowing)

Data la mole di dati – estremamente delicati – a cui abbiamo accennato, nasce il problema di **qualificare l'OdV ai sensi del G.D.P.R.,** ossia come titolare, responsabile o mero incaricato al trattamento. Questo rileva per stabilire la **responsabilità dei membri dell'OdV.**

A seconda della qualificazione giuridica, infatti, muta anche il titolo della responsabilità.

TITOLARE: in tal caso l'OdV dovrebbe porre in essere tutte le misure organizzative e di *compliance* previste dal G.D.P.R. Si troverebbe pertanto nell'obbligo di adottare un registro dei trattamenti, organizzare e gestire i flussi di dati, garantirne la sicurezza, effettuare una DPIA, nominare un DPO, segnalare un data breach…

RESPONSABILE: se così qualificato, l'OdV dovrebbe agire conformemente alle istruzioni fornite dal titolare del trattamento, che in questo caso sarebbe la società, perdendo così il ruolo di autonomia e indipendenza che gli è proprio...

Sul punto, il Garante ritiene che:

«Quanto alla qualifica come **titolare**: l'OdV non può essere autonomo titolare del trattamento, considerato che i suoi compiti di iniziativa e controllo non sono determinati dall'organismo stesso, bensì dalla legge che ne indica i compiti e dall'organo dirigente che nel modello di organizzazione e gestione definisce gli aspetti relativi al funzionamento compresa l'attribuzione delle risorse, i mezzi e le misure di sicurezza (art. 6, commi 1 e 2 d.lgs. n. 231/2001).

Quanto alla qualifica come **responsabile**: l'OdV non può essere considerato tale in quanto non si tratta di ente distinto dal titolare. Nel caso dell'OdV, eventuali omessi controlli in ordine all'osservanza dei modelli predisposti ricadono semplicemente sull'ente stesso.»

"Sulla base delle valutazioni sopra riportate, si ritiene che l'OdV, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongono siano interni o esterni, debba essere considerato **"parte dell'ente".**

Il suo ruolo - che si esplica nell'esercizio dei compiti che gli sono attribuiti dalla legge, attraverso il riconoscimento di "autonomi poteri di iniziativa e controllo" - si svolge **nell'ambito dell'organizzazione dell'ente, titolare del trattamento, che, attraverso la predisposizione dei modelli di organizzazione e di gestione, definisce il perimetro e le modalità di esercizio di tali compiti.**

Lo stesso ente, nell'ambito dei compiti e delle funzioni affidate all'OdV, designerà - nell'ambito delle misure tecniche e organizzative da porre in essere in linea con il principio di accountability (art. 24 del Regolamento) - **i singoli membri dell'OdV quali soggetti autorizzati** (artt. 4, n. 10, 29, 32 par. 4 Regolamento; v. anche art. 2-quaterdecies del Codice).

Tali soggetti, in relazione al trattamento dei dati degli interessati, dovranno attenersi alle istruzioni impartite dal titolare affinché il trattamento avvenga in conformità ai principi stabiliti dall'art. 5 del Regolamento.

Lo stesso titolare sarà tenuto ad adottare le misure tecniche e organizzative idonee a garantire la protezione dei dati trattati, assicurando contestualmente all'OdV l'autonomia e l'indipendenza rispetto agli organi di gestione societaria nell'adempimento dei propri compiti secondo le modalità previste dalla citata normativa".

ODV E WHISTLEBLOWING – GDPR: L'INTERPRETAZIONE DEL TAVOLO CONGIUNTO GDPR ORDINI DI TORINO (GIUGNO 2020)

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

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?)

ATTENZIONE!!!! Sono effettivamente iniziati i controlli e sono state applicate le prime sanzioni….

RECENTI E IMPORTANTI DECISIONI DELL'AUTORITA' GARANTE E DELL'AUTORITA' GIUDIZIARIA

- **Telemarketing aggressivo. Dal Garante privacy sanzione a Vodafone per 12 milioni 250 mila euro**

Il Garante per la protezione dati personali **ha ordinato a Vodafone il pagamento di una sanzione di oltre 12 milioni e 250 mila euro** per aver trattato in modo illecito i dati personali di milioni di utenti a fini di telemarketing.

L'Autorità ha quindi ordinato a Vodafone di introdurre dei sistemi che consentano di comprovare che i trattamenti a fini di telemarketing si svolgano nel rispetto delle disposizioni in materia di consenso. La società dovrà inoltre dimostrare che i contratti siano attivati solo a seguito di chiamate promozionali effettuate dalla sua rete di vendita, attraverso numerazioni censite e iscritte al Roc.
Vodafone dovrà anche irrobustire le misure di sicurezza al fine di impedire accessi abusivi ai database dei clienti e fornire pieno riscontro alle richieste di esercizio dei diritti formulate da alcuni utenti.

Il Garante, infine, ha vietato a Vodafone ogni ulteriore trattamento di dati con finalità promozionali o commerciali svolto mediante l'acquisizione di liste anagrafiche da soggetti terzi, senza che questi ultimi abbiano acquisito un consenso specifico, libero e informato dagli utenti per la comunicazione dei loro dati.

- **Il Garante privacy sanziona Eni Gas e Luce per 11,5 milioni**

  Telemarketing indesiderato e attivazione di contratti non richiesti

Il Garante per la privacy ha applicato a Eni Gas e Luce (Egl) due sanzioni, per complessivi 11,5 milioni di euro, riguardanti rispettivamente trattamenti illeciti di dati personali nell'ambito di attività promozionali e attivazione di contratti non richiesti.

Il Garante, dopo aver dichiarato l'illiceità delle condotte rilevate, ha ingiunto a Egl di implementare procedure e sistemi per verificare, anche tramite l'esame di un campione rilevante di nominativi, lo stato dei consensi delle persone inserite nelle liste dei contatti, prima dell'inizio delle campagne promozionali. Egl dovrà inoltre provvedere alla definitiva automatizzazione dei flussi di dati dal proprio database alla black list di chi non vuole ricevere pubblicità in uso presso la società.
Il Garante, inoltre, ha vietato alla società l'uso dei dati forniti dai list provider senza che questi ultimi avessero acquisito uno specifico consenso alla loro comunicazione a Egl.

Il Garante quindi, rilevate le irregolarità, ha ingiunto a Egl l'adozione di una serie di misure correttive e l'introduzione di specifici alert in grado di individuare varie anomalie procedurali.
Le implementazioni dovranno essere introdotte e comunicate all'Autorità in tempi stabiliti, mentre il pagamento delle sanzioni dovrà essere effettuato entro trenta giorni.

- **Avvocato invia lettere di convocazione ai condomini riutilizzando fogli già stampati sul retro con dati personali di altri clienti**

Per inviare delle convocazioni agli inquilini di una proprietà immobiliare, in almeno due casi una professionista legale non si è accorta che stava usando fogli che erano già stati stampati precedentemente e che nel retro contenevano informazioni personali di precedenti clienti, uno dei quali minorenne.

L'autorità ha quindi preso atto che la professionista aveva effettivamente commesso una violazione dell'art. 32 del Gdpr, che obbliga i titolari del trattamento a mettere in atto "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*", che comprendono la "*capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*" nonché una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Per tali motivi, pur riconoscendo che si fosse trattato di una negligenza involontaria, il garante spagnolo ha comunque constatato che le informazioni che apparivano sul retro dei documenti "*sono dati personali che consentono l'identificazione delle persone interessate*", e pertanto con procedimento N.PS/00390/2019 del 9 giugno 2020 ha inflitto una multa di 2.000 euro alla professionista.

- **Irlanda: dati sanitari smaltiti in un centro di riciclaggio pubblico, multato l'ospedale**

Dati personali di 78 pazienti dell'Ospedale di maternità della Cork University sono stati scoperti mentre venivano smaltiti in una struttura di riciclaggio pubblica

Trattandosi di informazioni sensibili rientranti nelle particolari categorie di dati ai sensi dell'art. 9 del Gdpr, dalla loro esposizione può essere derivato un impatto significativo sui diritti e le libertà degli interessati, e potrebbero essere state potenzialmente utilizzate anche utilizzate contro di loro in modo discriminatorio, ragion per cui l'autorità di controllo per la protezione dei dati irlandese (Data Protection Commission) ha stabilito che l'Ospedale della Cork University abbia violato gli articoli 5 e 32 del Gdpr "*non avendo implementato misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio presentato dal suo utilizzo e smaltimento di documenti cartacei contenenti dati personali dei pazienti* ", e per tali motivi ha inflitto una sanzione di 65mila euro all'ospedale, il quale ha accettato il provvedimento senza proporre ricorsi.

• Twitter: verdetto in arrivo dai Garanti Privacy dell'UE

Con l'introduzione del nuovo Regolamento UE sulla protezione dei dati personali, due anni e mezzo fa Twitter e la maggior parte dei giganti del web avevano infatti approfittato della regola del "*one stop shop*", che consentiva loro di stabilire la propria sede europea in Irlanda per avere a che fare con una sola "*autorità capofila*" per la privacy, che in molti casi sarebbe coincisa con quella di una nazione già per loro vantaggiosa anche dal punto di vista fiscale.

I fatti risalgono al gennaio del 2019, quando emerge che una parte di utenti del noto social di microblogging che vogliono tutelare maggiormente la loro privacy impostano la funzione "Proteggi i tuoi tweet", ma proprio così facendo i loro dati personali vengono invece esposti a loro insaputa a rischio di violazioni a causa di un bug esistente fin dal 2014.

Ma poiché nel frattempo è entrato in vigore il Gdpr, Twitter avrebbe dovuto notificare il "data breach" al garante irlandese entro 72 ore dal momento della scoperta, adempimento che a quanto pare non viene espletato così tempestivamente dalla società americana.

La questione è stata definita al tavolo dell'European Data Protection Board, innescando in tal modo un complesso meccanismo di risoluzione delle controversie previsto dall'art.65 del Regolamento UE 2016/679, che **il 9 novembre 2020** è sfociato, per la prima volta da quando è entrato in vigore il Gdpr, in una decisione vincolante adottata a maggioranza dei due terzi dei membri del comitato delle autorità europee.

- **Corte di Cassazione Penale, sentenza n. 41604 del 10 ottobre 2019**

In tema di trattamento illecito dei dati personali, l'invio a una vasta platea di utenti di più messaggi di posta elettronica non desiderati non dà luogo al nocumento previsto come elemento costitutivo del reato di cui all'art. 167 d.lgs. 30 giugno 2003, n. 196, in quanto lo stesso non può esaurirsi nel semplice fastidio di dover cancellare, di volta in volta, tali mail, ma deve tradursi in un pregiudizio concreto, anche non patrimoniale, suscettibile comunque di essere oggettivamente apprezzato. (Fattispecie in cui la Corte ha annullato senza rinvio una sentenza di condanna in un caso nel quale i componenti di un'associazione, dopo aver ricevuto pochi messaggi pubblicitari di posta elettronica, non avevano comunicato al mittente la volontà di non riceverne altri e, comunque, quest'ultimo non aveva perseverato nell'inviarli, chiarendo che il nocumento deve desumersi dalla quantità dei messaggi spediti a ciascun associato e non dal numero di quelli complessivamente inviati alla totalità di essi).

Si è, dunque, ribadito che perché sussista il reato è necessaria la prova del DOLO SPECIFICO e del NOCUMENTO

- **Corte di Cassazione Civile, sentenza n. 18292 del 3 settembre 2020**

COMUNE DIFFONDE I DATI PERSONALI DI UNA DIPENDENTE

In tema di protezione dei dati personali, ai sensi dell'art. 28 del d.lgs. n. 196 del 2003 il titolare del trattamento è la persona giuridica e non il suo legale rappresentante o l'amministratore, venendo in rilievo un'autonoma responsabilità in deroga al principio dell'imputabilità personale della sanzione di cui alla l. n. 689 del 1981. Tale responsabilità è fondata sul concetto di "colpa di organizzazione", da intendersi, in senso normativo, come rimprovero derivante dall'inosservanza da parte dell'ente dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenire la commissione degli illeciti.

Il «tavolo di lavoro congiunto GDPR»
dei nostri Ordini Professionali
è al fianco dei colleghi.

GRAZIE

PAOLA ZAMBON – DOTTORE COMMERCIALISTA - REFERENTE GDPR ORDINE COMMERCIALISTI

CLAUDIO STRATA – AVVOCATO – REFERENTE GDPR ORDINE AVVOCATI

PAOLO TRAVERSA - INGEGNERE - REFERENTE GDPR ORDINE INGEGNERI

TaxLawPlanet™ Webinar