ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Privacy 2018

(seconda parte)

Il responsabile della protezione dei dati (DPO – Data Protecion Officer)

Alberto Baj Macario

4 Maggio 2018 Odcec Sala Convegni Corso Europa 11 Milano

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Responsabile della protezione dei dati
DPO

Fonti del diritto:

GDPR (general data protection regulation)
Art. 37-38-39
Comitato europeo per la protezione dei dati
Autorità di controllo

WP29 ex 95/46/CE per le indicazioni

INDICAZIONI

Il lamento degli addetti:

Tali fonti di diritto non sono delle regole ma sono dei principi che diventano degli adempimenti.

(che hanno sanzioni gravissime)

COMPITI

- Dovere d'informazione, consulenza, responsabilizzazione, sensibilizzazione del titolare, responsabile del trattamento e dipendenti svolgenti il trattamento;
- Sorveglianza GDPR, delle leggi e delle politiche del titolare;
- Fornire un parere sul PIA (valutazione d'impatto sulla protezione dei dati) (Atr. 35);
- Essere il contatto per l'autorita di controllo per la consultazione preventiva (ART. 36)

Nei compiti considera

<u>debitamente i rischi del trattamento</u>

tenendo conto la natura, ambito di applicazione, contesto e finalità del trattamento.

Funzione consultiva e di controllo

- Ha il diritto e dovere di essere coinvolto tempestivamente in tutte le questioni riguardanti la protezione dei dati (Art. 38) [considerazioni del GDPR 77]
- Nelle informazioni da dare all'interessato occorre indicare il contatto del DPO (art. 13 e 14);
- Viene richiamato nel registro delle attività dei trattamenti (art. 30);
- Viene richiamato nella notifica all'autorità di controllo (art 33) come punto di contatto;

Obbligo di designazione

- Per il trattamento svolto da autorità pubblica, eccetto magistratura;
- Se l'attività principale del titolare consiste nel trattamento di dati, per natura e ambito, derivanti dal monitoraggio regolare e sistematico degli interessati su larga scala (art. 9);
- Se l'attività principale del titolare consiste nel trattamento su larga scala di dati particolari (art.9) e dati relativi a condanne penali e reati (art. 10);
- ovvero da singoli casi imposti dalla legge nazionale e dalla UE;
- ovvero su base volontaria;

Cosa significa attività principale

Nel WP 243 (linea guida) del gruppo di lavoro Art 29 95/46/CE anche WP29:

L'attività principale è strettamente connessa con il trattamento dei dati. In un ospedale il trattamento dei dati relativi alla salute è sicuramente una attività principale.

Non è attività principale il trattamento di informazioni relative al proprio personale in quanto accessoria all'attività.

Cosa significa "su larga scala"

Nel WP 243 (linea guida) del gruppo di lavoro Art 29 95/46/CE anche WP29:

- Il numero di soggetti trattati in termini assoluti ovvero in proporzione alla popolazione di riferimento;
- Il volume e/o le diverse tipologie di dati;
- La durata e/o la persistenza dell'attività di trattamento;
- La portata geografica del trattamento;

Trattamento dei pazienti in un ospedale – utenti di un servizio pubblico di trasporto – geolocalizzazione per finalità statistiche – trattamento di dati assicurativi e bancari nelle loro attività- motore di ricerca per finalità di pubblicità comportamentale.

Non è su larga scala il trattamento di uno studio di avvocati e di un singolo medico.

Monitoraggio regolare e sistematico

Nel WP 243 (linea guida) del gruppo di lavoro Art 29 95/46/CE anche WP29:

Nel 'considerando' 24 si richiama il "monitoraggio del comportamento di detti interessati" che ricomprende tutte le forme di tracciamento e profilazione su Internet [e non solo].

Tuttavia nel criterio di scelta di cui all'art. 37 si richiama "il monitoraggio dell'interessato"

Attività di marketing basate sull'analisi di dati raccolti – profilazione e scoring – tracciamento delle ubicazioni-programmi di fidelizzazioni.

Valutare la nomina del DPO

Si consiglia sempre di documentare le valutazioni compiute per stabilire la necessità di nominare o di non nominare il DPO

Tale analisi fa parte della documentazione da produrre in base al principio della responsabilizzazione

Designazione del DPO

La nomina rigurada un unico DPO per tutti i trattamenti svolti dal titolare del trattamento o dal responsabile del trattamento.

<u>Attenzione:</u>

Vi possono essere dei casi in cui il titolare del trattamento non necessita del DPO mentre il responsabile esterno, che ha un numero elevato di clienti, a sua volta viene obbligato alla nomina del DPO

Il DPO puo:

Essere nominato unico in un gruppo imprenditoriale purché sia facilmente raggiungibile da ciascun stabilimento (in quanto punto di contatto con gli interessati e con l'autorita di controllo).

Essere nominato da più organismi pubblici tenendo tuttavia conto della struttura organizzativa.

Qualità professionali e specifiche DPO

Nel WP 243 (linea guida) del gruppo di lavoro Art 29 95/46/CE anche WP29:

IL DPO è designato in funzione delle qualità professionali

- specialistica della normativa;
- prassi in materia di protezione dei dati (nazionali ed europee);
- Capacità di assolvere i compiti;

Autonomia e conflitti di interesse del DPO

- Il DPO può essere un dipendente ovvero un prestatore di servizi professionali.
- Il titotlare/responsabile sostengono il DPO per i suoi compiti di cui all.art. 39.
- Il DPO riferisce direttamente al vertice gerarchico del titolare/responsabile
- Il DPO può svolgere altri compiti purché non diano adito a un conflitto d'interesse (non può definire le finalita e modalita del trattamento).

(con risorse necessarie per i compiti, e per accedere ai dati personali, trattamenti a mantenere la conoscenza specialistica)

Riepilogo attività DPO

Nel WP 243 (linea guida) del gruppo di lavoro Art 29 95/46/CE anche WP29:

Contribuisce a dare attuazione del GDPR;

Principi fondamentali del trattamento;

Diritti degli interessati

Protezione dei dati (in progettazione e per impostazione predefinita)

Registri dell'attività di trattamento;

Sicurezza trattamento;

Notifica violazioni;

Punto di contatto;

Da ricordarsi: il DPO verifica la propria nomina, la comunica all'Autorita di controllo e nelle comunicazioni di privacy, amministra il proprio ufficio/fondi, verifica periodica dell'attività svolta.