Data Privacy Officer

A cura di:

Francesca Scarazzai e Cristina Chiantia

Dottori Commercialisti

Politecnico di Torino – 18 novembre 2

La figura del Data Protection Officer (DPO)

Figura già prevista dall' Art. 24 c. 1 Reg. 45/2001/CE : «Ogni istituzione ed organismo della Comunità è tenuto a nominare almeno un *responsabile della protezione dei dati personali*»

Conosciuto nel mondo anglosassone come *Chief Privacy Officer* (CPO), *Privacy Officer*, *Data Protection Officer*, *Data Security Officer*

Ora introdotto dal Regolamento generale sulla Protezione dei Dati (GDPR – General Data Protection Regulation) 2016/679 pubblicato sulla Gazzetta Ufficiale europea L.119 del 04/05/2016

Art. 37 del GDPR: Designazione

- Designazione obbligatoria da parte del titolare o del responsabile del trattamento quando [cit. GDPR]:

«a) il trattamento è effettuato da un'autorità pu… da un organismo pubb… cettuate le autorità giurisdizionali quando esercitano le loro …zioni giurisdizionali;

*b) **le attività principali del titolare del trattamento o del responsabile del trattamento** consistono in trattamenti che, per loro natura, ambito di applicazio… e/o finalità, richiedono il monitoraggio regolare e sist…matico degli interessati su larga …la;*

*c) **le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala,** di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.»*

Art. 37 del GDPR: Designazione

- Designazione obbligatoria da parte del titolare o del responsabile del trattamento quando [cit. Scheda informativa predisposta dal Garante]: :

*«a)**amministrazioni ed enti pubblici**, fa[illegible]zione per le autorità giu[illegible]rie;*

*b)tutti i soggetti la cui **attività principale** co[illegible]siste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il **controllo regolare e sistematico degli interessati**;*

*c)tutti i soggetti la cui **attività principale** co[illegible] trattamento, su [illegible] di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.»*

- Designazione facoltativa anche in casi diversi da quelli sopra indicati.
- Designazione da parte di un gruppo di imprese o soggetti pubblici : possono nominare un **unico Responsabile della protezione dei dati**.

Art. 37 del GDPR: Designazione

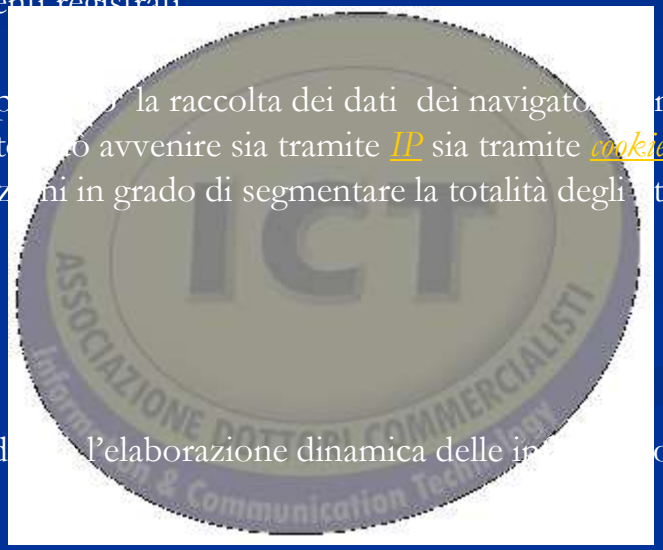
- Designazione obbligatoria per:
  - ENTI PUBBLICI, PUB[illegible]CHE AMMINISTRAZIONI [illegible]ENTRALI O LOC[illegible]ALI
  - PRIVATI:
    - settore sanitario, elabora[illegible]zione paghe, ….
    - settori in cui sono poste [illegible]essere attività di pr[illegible]zione su larga scala

Si richiede intervento esplicativo da parte del Garante

Profiling

Profiling esplicito: Prevede la *procedura di registrazione*, che implica la fornitura di *dati personali* da parte dell'utente. Ai dati personali, archiviati e conservati, verranno successivamente abbinate altre informazioni . Tutti i dati inviati vengono utilizzati per *segmentare* in gruppi omogenei gli utenti registrati.

Profiling implicito : Non prevede alcuna registrazione p[illegible] la raccolta dei dati dei navigato[illegible]no relativi ai loro comportamenti durante la navigazione. Il tracciament[illegible]o avvenire sia tramite *IP* sia tramite *cookie*. L'insieme dei comportamenti vengono utilizzati per derivare correlaz[illegible]ni in grado di segmentare la totalità degli [illegible]tenti tracciati in *gruppi omogenei*.



- **Esempi:**

1. Profilazione della clientela

- Creazione dei profili comportamentali dei clienti med[illegible]l'elaborazione dinamica delle in[illegible]oni raccolte al fine di potergli rivolgere un'offerta mirata,.

2. Profilazione del mercato

- Consiste nella mappatura del mercato nel quale si opera e nell'analisi del suo posizionamento : consente l'analisi della concorrenza, dei fattori strategici oltre che l'identificazione della propria clientela potenziale.

3**. Profilazione delle risorse umane**

- Consente la valutazione delle risorse umane (potenzialità , motivazione, soddisfazione) e la identificazione di caratteristiche tipiche e caratterizzanti i diversi ruoli professionali e categorie produttive.

Art.38 del GDPR: Posizione

Il titolare ed il responsabile del trattamento devono:

a) Coinvolgere ed informare tempestivamente il DPO
b) Sostenerlo nell'esecuzione dei suoi c[illegible] (art.39) fornendogl[illegible]isorse necessarie per assolvere i suoi compi[illegible]accedere ai dati e ai trattam[illegible]nti, mantenere le proprie conoscenze sp[illegible]cialistiche
c) Garantirne e tutelarne l'autonomia (il DPO riferisce direttamente al vertice gerarchico del titolare o del responsabile del trattamento)

Il DPO:

1. può essere contattato dall'interessato per tutte le questioni relative ai propri dati personali
2. È tenuto alla riservatezza
3. Può svolgere altri compiti e funzioni in assenza di conflitti di interesse

Art.39 del GDPR: Compiti

Il DPO deve:

- informare e consigliare sull' osservanza del GDPR e di tutte le altre disposizioni,
- controllare e vigilare sull' osservanza del GDPR e di tutte le altre disposizioni,
- controllare e vigilare sulle politiche del titolare e del responsabile del trattamento in materia di trattamento dei dati, attribuzione delle responsabilità, formazione e sensibilizzazione del personale e sull' audit connesso,
- fornire un supporto strategico se richiesto, fornire una valutazione di impatto sulla protezione dei dati [PIA – Privacy Impact Assessment] ex art. 35) – possibile coinvolgimento anche nel DATA PROTECTION BY DESIGN ex art.25 ?)
- agire in rappresentanza nei confronti delle autorità di controllo.

Quali sono le expertise che deve possedere?

- Dottore Commercialista o altro professionista che abbia maturato esperienza come consulente privacy
- Esperto nella legislazione U[illegible]ulla privacy (no[illegible]né art. 16 trattato funzionamento [illegible]E, art. 8 Carta diritt[illegible] umani)
- Comprensione su tipo di dati e contesto in cui o[illegible]era
- Tre anni di esperienza com[illegible] responsabile del trattamento in un ente che [illegible]n tratta i dati p[illegible]nali come core business
- Sette anni di esperienza come responsabile del trattamento in un ente che tratta i dati personali come core business o a scopo commerciale

Best practice

- Almeno una o due volte l'anno deve preparare un Report che informi sullo stato di conformità dell'ente
- All'inizio di ogni anno deve presentare un piano di lavoro programmatico delle attività da svolgere
- Deve essere coinvolti nelle discussioni in cui si tratta di dati personali
- Per gli enti EU più grandi dovrebbe essere previsto un incontro tra responsabili per fare network