ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Privacy 2018

Parte prima

Le figure soggettive del trattamento (titolare, contitolare, responsabile, sub-responsabile) e le relative responsabilità

LAURA SALAMONE
Commissione Informatica, CCIAA e Registro Imprese di Milano
G.d.L Privacy

6 aprile 2018, corso Europa 11 – Milano

Definizioni (art. 4 par. 7 e 8)

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

Responsabile

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

Le figure soggettive del trattamento

Titolare (art. 24)

↓

Contitolare (art. 26)

Responsabile (art. 28)

↓

Sub - responsabile (art. 28, par. 2)

Titolare del trattamento (art. 24)

Responsabilità

Nuove disposizioni in materia di privacy di cui al Regolamento UE n. 2016/679

"principio di **responsabilizzazione**".

Accountability

PRINCIPIO DI RESPONSABILIZZAZIONE (ACCOUNTABILITY)

Il Titolare e il Responsabile per conto del Titolare

<u>devono</u>

essere in grado di "dimostrare" e "comprovare" il rispetto dei principi del GDPR .

Il principio di responsabilizzazione

- **Centralità** dei titolari e responsabili del trattamento nella pluralità di soggetti coinvolti;
- **Criterio d'interpretazione:** criterio non formale; adempimenti vs. strumenti per l'adempimento;
- Attuazione del GDPR come **"generatore di prassi"**
- **Dinamicità** nell'attuazione del GDPR: il soggetto interessato; dai dati comuni ai dati sensibili;
- Linee guida, standards, checklist > **roadmap**
- Presupposti della roadmap: **ricognizione interna.**

Roadmap: ricognizione interna

Ricognizione interna in ordine di importanza

1. RISORSE (umane ed economiche: viene meno il paradigma della gestione a risorse invariate)

2. COMPETENZE (formazione del personale)

3. INFRASTRUTTURE (informatiche/documentali)

4. DATI (tipologie di dati per ciascun trattamento: qualità dei dati = accuratezza e aggiornamento)

5. TRATTAMENTI (differenti tipologie di trattamenti di dati per ciascun ambito)

Responsabilità solidale (art. 82)

Il Responsabile è responsabile in solido con il Titolare

per l'intero ammontare dell'eventuale danno causato dal trattamento, al fine di garantire l'effettivo risarcimento dell'interessato

Responsabilità solidale (art. 82)

L'eventuale azione di regresso sarà possibile se il Responsabile

- non ha adempiuto agli obblighi del GDPR
- ha agito in modo difforme o contrario rispetto alle istruzioni formalizzate nel contratto

culpa in eligendo e culpa in vigilando

Titolare del trattamento (art. 24)

Mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è stato effettuato conformemente al GDPR

Le misure debbono essere periodicamente riesaminate e aggiornate qualora necessario

Titolare del trattamento (art. 24)

Attuazione di politiche adeguate in materia di protezione dei dati

Un meccanismo di certificazione approvato ex art. 42 può essere utilizzato come elemento per dimostrare la conformità a detti requisiti

Titolare del trattamento (art. 24)

Obblighi del Titolare

Il Titolare deve sempre specificare:

- la propria identità e quella dell'eventuale rappresentante nel territorio italiano
- le finalità del trattamento
- i diritti degli interessati
- se esiste un responsabile del trattamento e la sua identità
- quali sono destinatari dei dati

Responsabilità del titolare del trattamento (art. 25)

Par. 1

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i **diritti e le libertà delle persone fisiche**,

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 presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Responsabilità del titolare del trattamento

Adempimenti

- Privacy by design e by default (art. 25)
- Registro delle attività di trattamento (art. 30)
- Sicurezza del trattamento (misure adeguate), (art. 32)
- Notifica delle violazioni di dati personali [data breaches] (art. 33) Valutazione d'impatto sulla protezione dati (DPIA), (art. 35)
- Responsabile per la protezione dei dati (DPO), (art. 37 e 39)

Linee guida per gli adempimenti

- DPIA/Privacy by design e by default
- Art. 29 WP, Statement on the role of a risk-based approach in data protection legal framework, 14/EN 218;
- Art. 29 WP, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk", 17/EN 248;
- Guida all'applicazione del Regolamento, Garante Privacy
- ISO/IEC 29134 - Information technology – Security techniques – Guidelines for PIA;
- CNIL [Commission Nationale de l'Informatique et des Libertés] – DPIA – PIA
- ICO (Information Commissioner's Office) – Conducting privacy impact assessment – code of conduct
- ISO 31000 – Gestione del rischio - Principi e linee guida
- ENISA (European Union Agency for Network and Information Security) Privacy and Data Protection by Design, 2015

Misure di sicurezza

- ISO/IEC 27001- Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti

- ISO/IEC 27005 - Information technology – Security techniques – Information security risk management NIST (National Institute of Standards and Technology) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organization

Adempimenti

Registro dei trattamenti

DPO

Art. 29 WP Guidelines on Data Protection officer 16/EN WP 243

Contitolare del trattamento (art. 26)

Determinazione congiunta delle finalità e dei trattamenti

Due o più Titolari → Contitolari

Accordo interno

determinazione delle rispettive responsabilità in merito all'osservanza degli obblighi derivanti

Titolare del trattamento (art. 24)

Il titolare effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali

L'art. 35 introduce la nozione di valutazione di impatto sulla protezione dei dati
("DPIA", Data Protection Impact Assessment, oppure "PIA", Privacy Impact Assessment)

cfr linee guida del WP art. 29

Titolare del trattamento (artt. 24 e 35)

L'obbligo di condurre una DPIA (in determinate circostanze) deve essere collocato nel contesto del più generale obbligo imposto ai titolari di gestire correttamente i rischi connessi al trattamento di dati personali.

"rischio": uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità;

"gestione del rischio": l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente nei riguardi di tale rischio.

Responsabile del trattamento (art. 28)

Scelta del responsabile

- Il titolare del trattamento potrà servirsi di responsabili del trattamento solo se fornisce garanzie sufficienti ad adottare misure tecniche e organizzative adeguate.
- Contratto sul trattamento in forma scritta (previsti modelli di contratto).

Delega del trattamento

- Il responsabile del trattamento non può ricorrere a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.
  Il responsabile iniziale conserva nei confronti del titolare l'intera responsabilità per l'adempimento degli obblighi dell'altro responsabile.

Responsabile del trattamento (art. 28)

Responsabilità

- **Azioni dirette:** l'interessato può presentare un reclamo direttamente contro il responsabile (in via amministrativa e giudiziale).

- **Responsabilità qualificata:** un responsabile è responsabile del danno cagionato dal trattamento solo se non ha osservato i suoi obblighi specifici ai sensi presente regolamento specificamente o ha operato al di fuori o contrariamente alle istruzioni legittime del titolare del trattamento.

Responsabile del trattamento (art. 28)

Responsabilità

- **Onere della prova:** un titolare o un responsabile del trattamento non è considerato responsabile se dimostra di non essere in alcun modo responsabile dell'evento che ha causato il danno.

- **Responsabilità solidale:** qualora un titolare o un responsabile del trattamento siano coinvolti nello stesso trattamento e siano responsabili per i danni cagionati dal trattamento, ciascuno di loro è ritenuto responsabile per l'intero danno, per assicurare il ristoro effettivo dell'interessato.

Responsabile del trattamento (art. 28)

Responsabilità

- **Responsabile dei responsabili delegati:** qualora tali responsabili non rispettino i propri obblighi relativi alla protezione dati, il responsabile originario rimane interamente responsabile nei confronti del titolare per l'esecuzione degli obblighi di tale altro responsabile

Responsabile del trattamento (art. 28)

Il Responsabile deve mettere disposizione del titolare le informazioni

Infatti, al responsabile l'art.28 par.3 del Regolamento richiede di:

- trattare i dati solo su istruzione documentata del titolare
- garantire che le persone autorizzate dal trattamento dei dati personali si siano impegnate alla riservatezza
- adottare le previste misure di sicurezza
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie "per dimostrare il rispetto degli obblighi" previsti dalla norma
- consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto eventualmente da questi incaricato.

Responsabile del trattamento (art. 28)

Formalizzato

Contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri

condizione necessaria per vincolare il responsabile del trattamento al titolare del trattamento.

Responsabile del trattamento (art. 28)

Contenuti dell'Atto

- Materia disciplinata
- Durata del trattamenti
- Natura e Finalità del trattamentoTipo di dati e categorie degli Interessati
- Obblighi e diritti del Titolare e del Responsabile

Modalità del trattamento con le misure tecniche ed organizzative adeguate a consentire il rispetto delle istruzioni impartite dal Titolare e delle disposizioni del GDPR

(art. 28 par. 3 del GDPR e art. 29 Codice Privacy novellato dalla Legge 167/2017)

Sub - responsabile (art. 28, par.2)

Responsabile del trattamento

↓

Autorizzazione scritta specifica o generale

↓

Il Responsabile informa il Titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento

Sub - responsabile (art. 28, par.2)

Il Responsabile del trattamento può ricorrere per l'esercizio di specifiche attività di trattamento ad un altro Responsabile previa autorizzazione scritta, specifica o generale, del Titolare.

Arrivederci