




Avv. Monica Gobbato
La Responsabilità Privacy nella
Nuvola, tra genio e sregolatezza
13 Ottobre 2017



**Si fa prima a dire
COSA NON E'
CLOUD**

**| IL NUOVO
| REGOLAMENTO
PRIVACY EUROPEO
| 27 MAGGIO 2016**

Al Cloud provider è affidata la conservazione dei dati caricati dall'utente, questo assume una veste rilevante quanto al trattamento ed alle misure di sicurezza da attuare dei dati personali e tale ruolo è stato oggetto di interesse da parte dei Garanti Privacy a livello nazionale ed internazionale.

Altro oggetto di dibattito è il ruolo che assume il Cloud provider nei processi cui sono sottoposti dati personali: esso può essere associato sia alla figura del titolare del trattamento sia a quella di responsabile, sia a quella di contitolare.

Ora si aggiunge il ruolo di DPO

Contitolari del trattamento

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. **Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.** Tale accordo può designare un punto di contatto per gli interessati.

Responsabile del trattamento

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Responsabile del trattamento

Il trattamento da parte di un responsabile del trattamento sono disciplinati **da un contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

- a) **tratti** i dati personali soltanto su istruzione documentata del titolare del trattamento;
- b) **garantisca** che **le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;**
- c) **adotti tutte le misure** richieste ai sensi dell'articolo 32;

g) su scelta del titolare del trattamento, **cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti**, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) **metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni**, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato

(...omissis)

10. Se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, **è considerato un titolare del trattamento in questione.**

DATA PROTECTION OFFICER



A proposito di ACCOUNTABILITY art.24

La nomina di un DPO e' da considerarsi uno strumento di Accountability come le valutazioni di impatto e il dover essere punto di riferimento per l'Autorità Garante e per gli interessati

In caso di non obbligatorietà del DPO o non volontarietà è comunque consigliabile designare dei Responsabili Interni od Esterni che si occupino di Protezione Dati.

E' fondamentale che non si crei CONFUSIONE sullo status, la designazione, e compiti. NON SI DEVONO CONFONDERE CON I DPO

• IL DPO E' OBBLIGATORIO QUANDO

- a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
- c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali **relativi a condanne penali e reati.**

- il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:
 - - il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
 - - il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
 - - la durata, ovvero la persistenza, dell'attività di trattamento;
 - - la portata geografica dell'attività di trattamento.

Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato”.

• MONITORAGGIO REGOLARE E SISTEMATICO

- Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il “*monitoraggio del comportamento di detti interessati*” ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

- Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo
 - con riguardo all'ambiente online,

• **L'aggettivo “regolare” ha almeno uno dei seguenti significati a giudizio del WP29:**

- - che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- - ricorrente o ripetuto a intervalli costanti;
- - che avviene in modo costante o a intervalli periodici.

Compiti del responsabile della protezione dei dati (C97)

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) **informare e fornire consulenza al titolare** del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) **sorvegliare l'osservanza del presente regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

Compiti del responsabile della protezione dei dati (C97)

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Registri delle attività di trattamento (C82)

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.

GRAZIE

**www.monicagobbato.it
Avv.monicagobbato@gmail.com**

