

# Le figure previste dal GDPR: ruoli e responsabilità

*Rosaria Deluca*

*Pisa, 22 maggio 2018*

- ❑ Titolare
- ❑ Contitolare
- ❑ Responsabile del trattamento dei dati
- ❑ Responsabile della protezione dei dati (RPD/DPO)
- ❑ Autorità
- ❑ Interessato

- ❑ 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 (art. 4 p.7).

- ❑ E' prevista l'ipotesi di contitolarità del trattamento:
  - ❑ Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento (art. 26 p.1).

- ❑ In caso di «contitolarità» del trattamento i titolari devono definire, tramite accordo interno, rispettivamente l'ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati (art. 26 p.1,2);
- ❑ L'accordo interno è messo a disposizione degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari che operano congiuntamente (art. 26 p.3).

- ❑ Il titolare del trattamento non stabilito nell'UE o il responsabile del trattamento deve designare per iscritto un rappresentante nell'UE (art. 27 p.1).

- ❑ L'obbligo di designazione non si applica:
  - ❑ al trattamento occasionale;
  - ❑ quando il trattamento non riguarda, su larga scala, dati sensibili o dati giudiziari;
  - ❑ quando è improbabile che presenti un rischio per gli Interessati;
  - ❑ alle autorità pubbliche o agli organismi pubblici (art. 27 p.2).

- ❑ La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4 p.8, art. 28).



- ❑ Deve avvenire unicamente con un contratto o altro atto giuridico che disciplina:
  - ❑ materia e durata del trattamento;
  - ❑ natura e finalità del trattamento;
  - ❑ tipo di dati personali e categorie di interessati;
  - ❑ obblighi e diritti del titolare del trattamento (art. 28 p.3).

## Il contratto vincola il responsabile a:

- ❑ trattare dati soltanto su istruzione documentata del titolare;
- ❑ garantire che le persone autorizzate al trattamento dati si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale alla riservatezza;
- ❑ adottare tutte le misure di sicurezza richieste ai sensi dell'art. 32;
- ❑ rispettare le condizioni per ricorrere a un sub-responsabile;
- ❑ assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- ❑ assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- ❑ cancellare o restituire tutti i dati e cancellare le copie esistenti alla fine del trattamento;
- ❑ mettere a disposizione del titolare le informazioni necessarie per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni del titolare o dell'Autorità Garante.

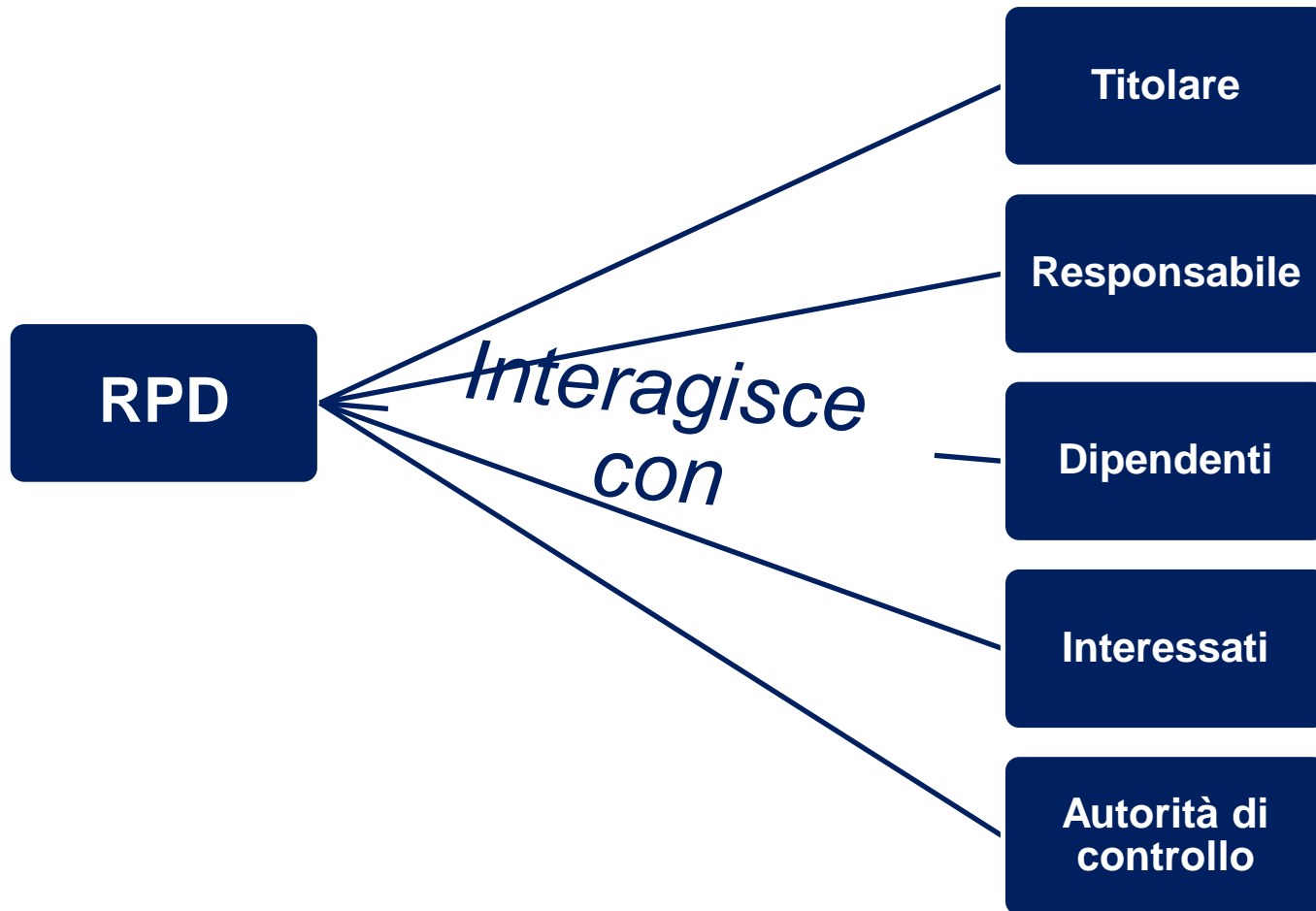
- ❑ Il contratto tra titolari e responsabili può basarsi, in tutto o in parte, su clausole contrattuali approvate dalla Commissione o da un'autorità Garante (art. 28 p.8).

- ❑ Il responsabile può nominare sub-responsabili per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e il primo responsabile (art. 28 p. 4).
- ❑ Il responsabile primario risponde dinanzi al titolare dell'inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile (art. 82 p.1,3).

# L'Incaricato?

- ❑ Il termine «Incaricato» non è menzionato, ma lo si evince dall'art. 4 p.10 che definisce terzo la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- ❑ Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri (art. 29).

# Responsabile protezione dati (RPD)



## □ *Fonti:*

- Considerando 97 GDPR, artt.37,38,39 GDPR;
- “Linee guida sui Responsabili della Protezione dei Dati (RPD)” del 13 dicembre 2016, predisposte dal “Gruppo di lavoro art. 29”, revisionate e pubblicate il 5 aprile 2017 (WP243).

- ❑ Trattamento effettuato da soggetti pubblici fatta eccezione delle autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali (art. 37 p. 1, a.);
- ❑ Più autorità pubbliche o organismi pubblici possono designare un unico RPD, tenuto conto delle dimensioni e della struttura organizzativa, purché sia facilmente raggiungibile da ciascuno stabilimento (art. 37 p.2).



# Obbligo di designazione del RPD...altri casi

- ❑ **Nel caso in cui le attività principali consistono in:**
  - ❑ trattamenti che per loro natura, ambito di applicazione e/finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, oppure
  - ❑ trattamenti su larga scala di categorie particolari di dati personali e dati relativi a condanne penali e a reati (art. 37 b,c).
- ❑ **Il significato di «larga scala» è stato specificato dal «Gruppo di lavoro art.29» in considerazione del:**
  - ❑ numero degli interessati;
  - ❑ massa di dati e tipologia di dati trattati;
  - ❑ durata del trattamento;
  - ❑ estensione geografica del trattamento (es: strutture sanitarie, aziende di trasporto, compagnie assicurative, istituti di credito, motori di ricerca, gestori telefonici, concessionari di servizi pubblici (es: fornitura gas, energia elettrica, ecc.)

## ❑ **Requisiti richiesti:**

- ❑ qualità professionali (esperienza professionale, formazione specialistica, certificazioni, etc. );
- ❑ conoscenza specialistica della normativa e della prassi in materia di protezione dei dati e delle normative di settore;
- ❑ capacità di assolvere i compiti assegnati (art. 37 a).

## ❑ **Alcune incertezze:**

- ❑ **RPD: interno od esterno?**
  - ❑ da valutare in base alla struttura,
  - ❑ se è esterno, la nomina deve essere regolata con un contratto di servizi.
- ❑ **RPD con competenze giuridiche o informatiche?**
  - ❑ competenze giuridiche ...ma il RPD dovrà interloquire con professionisti informatici.

- ❑ **art.38**
- ❑ coinvolgimento tempestivo e adeguato in tutte le questioni riguardanti la protezione dei dati personali;
- ❑ disponibilità di risorse economiche e organizzative per assolvere ai compiti affidati e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;
- ❑ garanzia di autonomia e indipendenza;
- ❑ nessuna penalizzazione o rimozione a causa delle funzioni;
- ❑ rapporto diretto con il vertice gerarchico;
- ❑ raggiungibilità per gli interessati;
- ❑ divieto di assegnazione di compiti e funzioni che risultano in conflitto di interessi.

- ❑ deve poter manifestare il proprio dissenso su decisioni ritenute non corrette.
- ❑ deve mantenere la riservatezza in merito alle attività svolte.
- ❑ la responsabilità di garantire e comprovare l'osservanza della normativa ricade sul titolare/responsabile del trattamento, tuttavia il RPD assume le responsabilità contrattuali nei confronti del titolare/responsabile.

- ❑ **art.39**
- ❑ informazione, consulenza e indirizzo al titolare e ai dipendenti;
- ❑ sorveglianza sull'osservanza della normativa sulla protezione dei dati (GDPR, norme nazionali e politiche in materia, regolamentazione interna adottata dal titolare o dal responsabile);
- ❑ formazione e sensibilizzazione dei dipendenti;
- ❑ fornire un parere in merito alla valutazione d'impatto della protezione dati (DPIA);
- ❑ cooperare con il Garante per la protezione dei dati personali;
- ❑ fungere da referente del Garante per la protezione dei dati.

## ❑ Comitato di controllo:

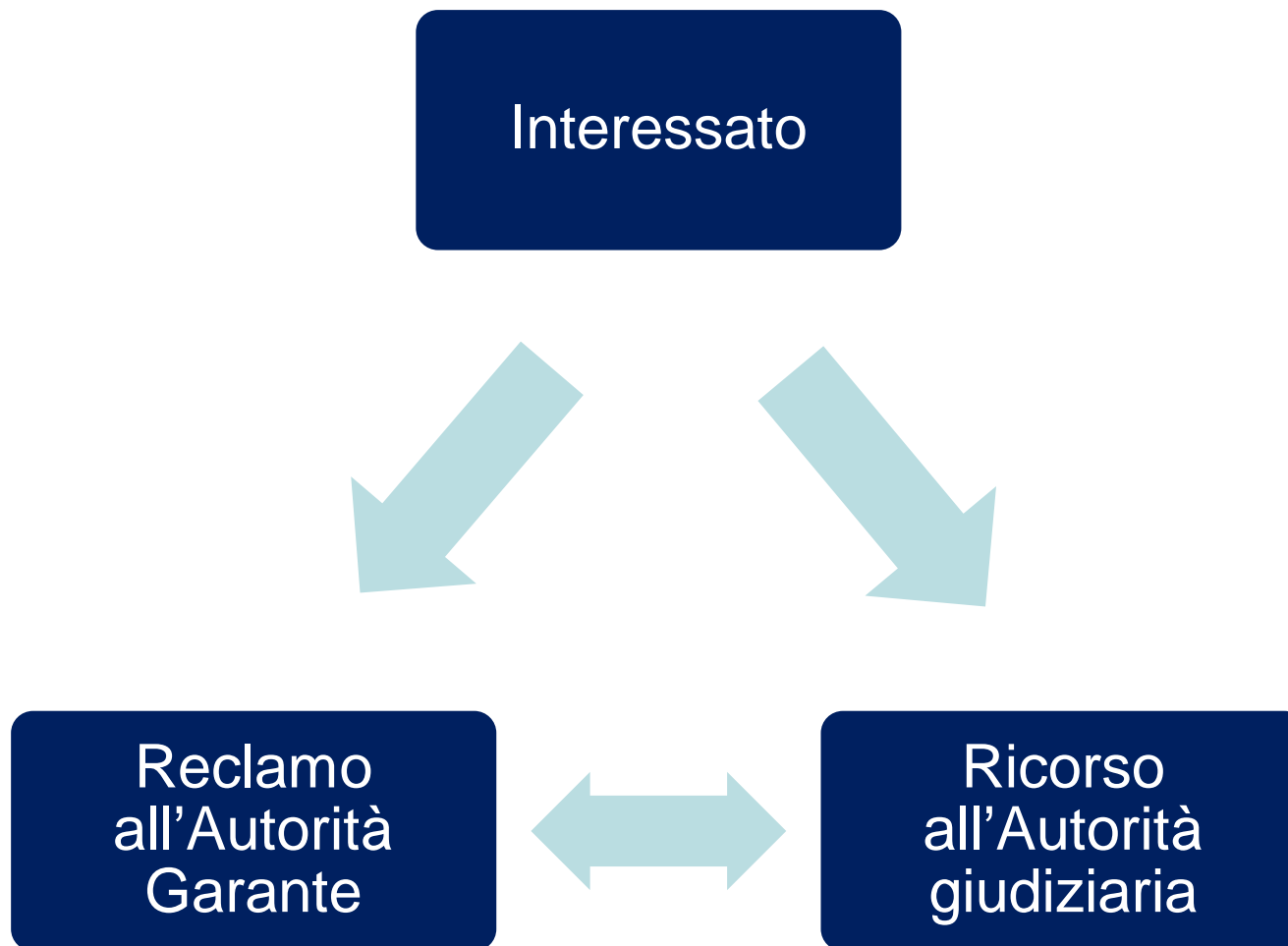
- ❑ organo europeo indipendente che assicura l'applicazione uniforme del Regolamento);
- ❑ sorveglia la corretta applicazione del Regolamento;
- ❑ emette pareri sui codici di condotta;
- ❑ pubblica linee guida;
- ❑ fornisce consulenza (artt.68-76).

## ❑ Autorità di controllo:

- ❑ l'Autorità pubblica indipendente istituita da uno stato membro (artt.51-59);
- ❑ in Italia corrisponde al Garante Privacy.

- ❑ L'Interessato è la persona fisica a cui si riferiscono i dati personali (art. 4 p.1), ...a cui la normativa attribuisce specifici diritti.









<http://stepnews.isti.cnr.it/>

*Grazie per l'attenzione!*