Evoluzione normativa: la figura del DPO. Le Linee-guida sul responsabile della protezione dei dati (RPD) adottate il 13 dicembre 2016 - versione emendata e adottata in data 5 aprile

Nomina, Posizione, Compiti

Avvocato Cristina Vicarelli

Regolamento DGPR, come scegliere il Responsabile della Protezione dei Dati - maggio 2018 non un vincolo ma un’opportunità.
- Napoli 6 novembre 2017-

Chi è il data protection officer?

siamo abituati a
titolare
responsabile
incaricato
(scansione gerarchica)

il DPO è un “facilitatore”

Chi nomina il DPO?
il titolare
o
il responsabile?

Nomina obbligatoria:

- ☑ trattamento svolto da PA (profilo soggettivo)
- ☑ **attività principale** richiede monitoraggio regolare o sistematico su **larga scala** (profilo oggettivo)
- ☑ **attività principale**: trattamento su **larga scala** di “categorie particolari di dati” (ex sensibili) o dati giudiziari (profilo oggettivo)
- ☑ **ulteriori ipotesi**: individuate dalla legislazione nazionale

Nomina facoltativa:

Se si procede alla nomina di un DPO su base volontaria, troveranno applicazione tutti i requisiti di cui agli artt. 37-39 per quanto concerne la nomina stessa, lo status e i compiti del DPO esattamente come nel caso di una nomina obbligatoria.

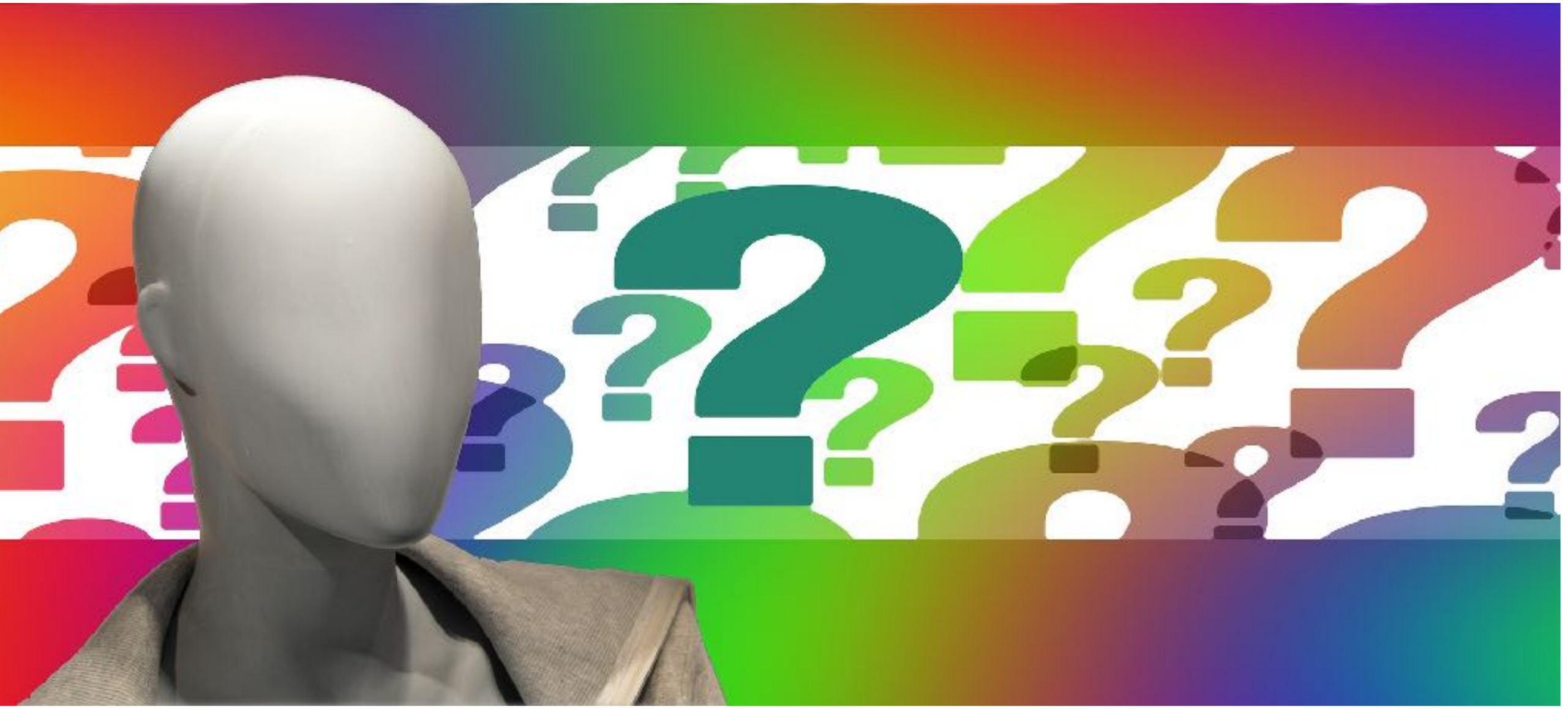
C’è un’altra possibilità:

Nulla osta a che un’azienda o un ente, quando non sia soggetta all’obbligo di designare un DPO e non intenda procedere a tale designazione su base volontaria, ricorra comunque a **personale o consulenti esterni** incaricati di incombenze relative alla protezione dei dati personali. In tal caso è fondamentale garantire che non vi siano ambiguità in termini di **denominazione**, **status** e **compiti** di queste figure; è dunque essenziale che in tutte le comunicazioni interne all’azienda e anche in quelle esterne (con l’autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti **non siano indicati con la denominazione di responsabile per la protezione dei dati (DPO)**.

Come faccio a sapere se sono obbligato o no a nominare un DPO?

Tranne quando sia evidente che un soggetto non è tenuto a nominare un DPO, il WP29 raccomanda a titolari e responsabili di **documentare le valutazioni** compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un DPO, **così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti**. Tale analisi fa parte della documentazione da produrre in base al **principio di responsabilizzazione**. Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario.

Chi devo nominare?



Conoscenze e competenze.
Soggetto interno o esterno?

Conoscenze e competenze specialistiche

- **conoscenza** della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa **un'approfondita conoscenza del RGPD**;
- **familiarità** con le operazioni di trattamento svolte;
- **familiarità** con tecnologie informatiche e misure di sicurezza dei dati;
- **conoscenza** dello specifico settore di attività e dell'organizzazione del titolare/del responsabile:
- **capacità** di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile.

Posizione del DPO

Posizione del DPO: 1. Coinvolgimento

- Il DPO deve essere tempestivamente ed adeguatamente coinvolto in tutte le questioni che riguardano la protezione dei dati personali

Coinvolgimento del DPO in tutte le questioni riguardanti la protezione dei dati personali

- Ai sensi dell'articolo 38 del RGPD, il titolare e il responsabile assicurano che il DPO sia "**tempestivamente** e **adeguatamente** coinvolto in tutte le questioni riguardanti la protezione dei dati personali".

- coinvolto **quanto prima** possibile in ogni questione attinente la protezione dei dati.

- PIA: coinvolgimento repentino tassativamente previsto,

- ciò facilita l'osservanza del RGPD e il rispetto del principio di privacy (e protezione dati) fin dalla fase di progettazione (= approccio standard).

- Inoltre, è importante che il DPO sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

Cosa significa in concreto?
Significa che è bene che:

- il DPO sia invitato a partecipare su base regolare alle **riunioni del management** di alto e medio livello;

- il DPO sia presente ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il DPO deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;

- il parere del DPO riceva sempre la dovuta considerazione. In caso di **disaccordi**, il WP29 raccomanda, quale buona prassi, di **documentare le motivazioni** che hanno portato a condotte difformi da quelle raccomandate dal DPO;

- il DPO sia consultato tempestivamente qualora si verifichi una **violazione** dei dati
  o un altro incidente.

- siano predisposte **linee guida**

Posizione del DPO:
2. Risorse necessarie

Risorse necessarie

- supporto attivo delle funzioni del DPO da parte del **senior management** (per esempio, a livello del consiglio di amministrazione);

- **tempo** sufficiente per l'espletamento dei compiti affidati al DPO. Ciò riveste particolare importanza se viene designato un DPO interno con un contratto part-time, oppure se il DPO esterno si occupa di protezione dati oltre a svolgere altre incombenze;

- supporto adeguato in termini di **risorse finanziarie, infrastrutture** (sede, attrezzature, strumentazione) e, ove opportuno, **personale**;

Risorse necessarie

- **comunicazione ufficiale della nomina del DPO a tutto il personale**, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'azienda/ dell'organismo;

- **accesso** garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al DPO supporto, informazioni e input essenziali;

- **formazione permanente**. I DPO devono avere la possibilità di curare il proprio aggiornamento con riguardo agli sviluppi nel settore della protezione dati.

Risorse necessarie

- Alla luce delle dimensioni e della struttura della singola azienda/ del singolo organismo, può risultare necessario **costituire un ufficio o un gruppo di lavoro DPO** (formato dal DPO stesso e dal rispettivo personale). In casi del genere, è opportuno **definire con precisione la struttura interna del gruppo** di lavoro nonché **i compiti** e le **responsabilità individuali**.

- Analogamente, se la funzione di DPO viene esercitata da un fornitore di servizi **esterno** all'azienda/all'organismo, potrà aversi la costituzione di un gruppo di lavoro formato da soggetti operanti per conto di tale fornitore e incaricati di svolgere le funzioni di DPO **sotto la direzione di un responsabile che funga da contatto per il cliente**.

Posizione del DPO:
3. Conflitto di interessi

Regolamento Generale sulla Protezione dei dati art. 38 - paragrafo 6

al DPO è consentito di "**svolgere altri compiti e funzioni**"

ma

a condizione che il titolare o il responsabile del trattamento si assicuri che "tali compiti e funzioni **non diano adito a un conflitto di interessi**"

il DPO non può rivestire, all'**interno dell'organizzazione** del titolare o
del responsabile, un ruolo che comporti

la definizione di

finalità

modalità

del trattamento di dati personali.

Esempi di conflitti

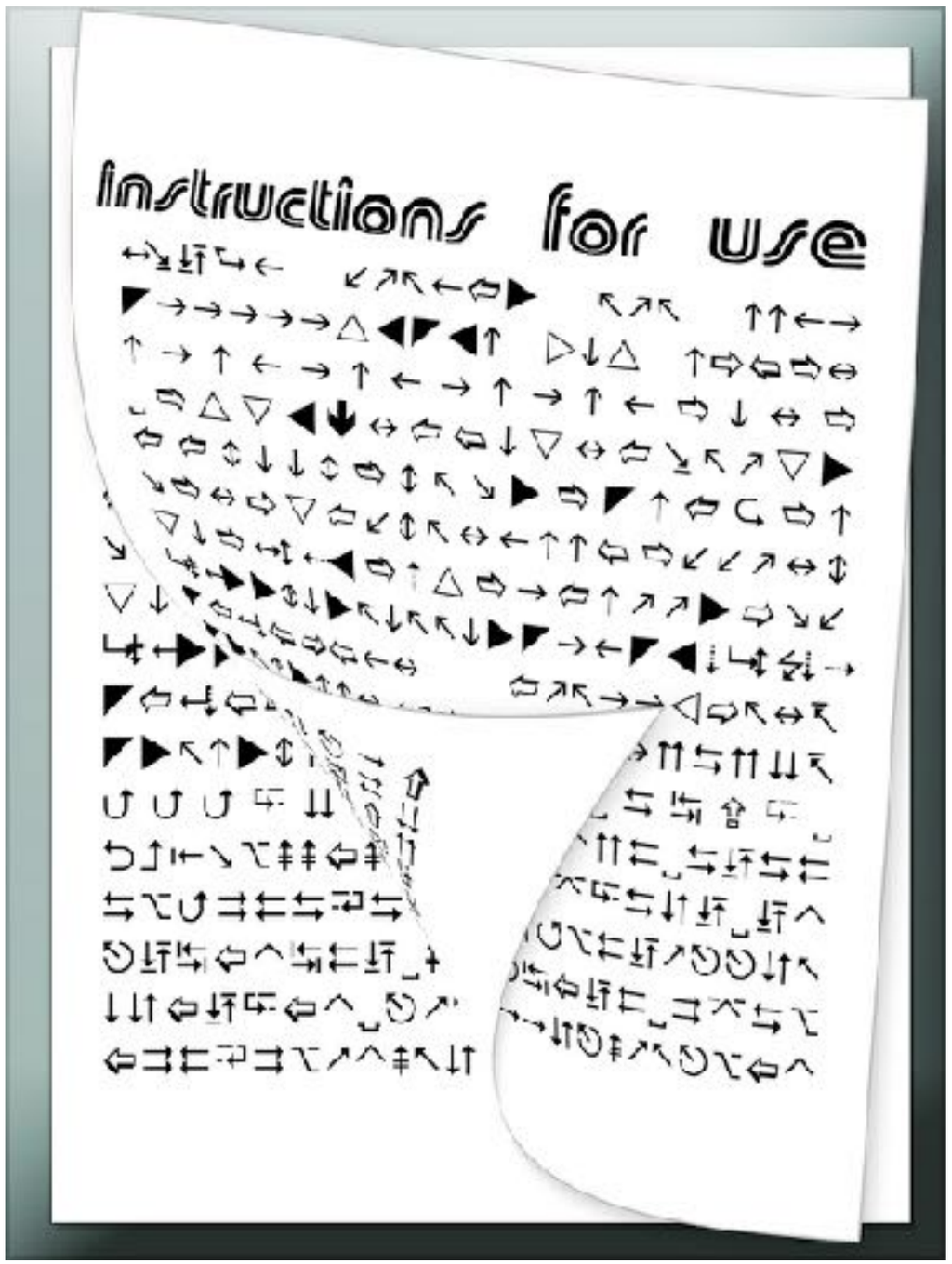
A grandi linee, possono sussistere situazioni di conflitto con riguardo a **ruoli manageriali di vertice** (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a **posizioni gerarchicamente inferiori** se queste ultime comportano la **determinazione** di **finalità** o **mezzi** del trattamento.

Posizione del DPO:
4. Istruzioni

Istruzioni

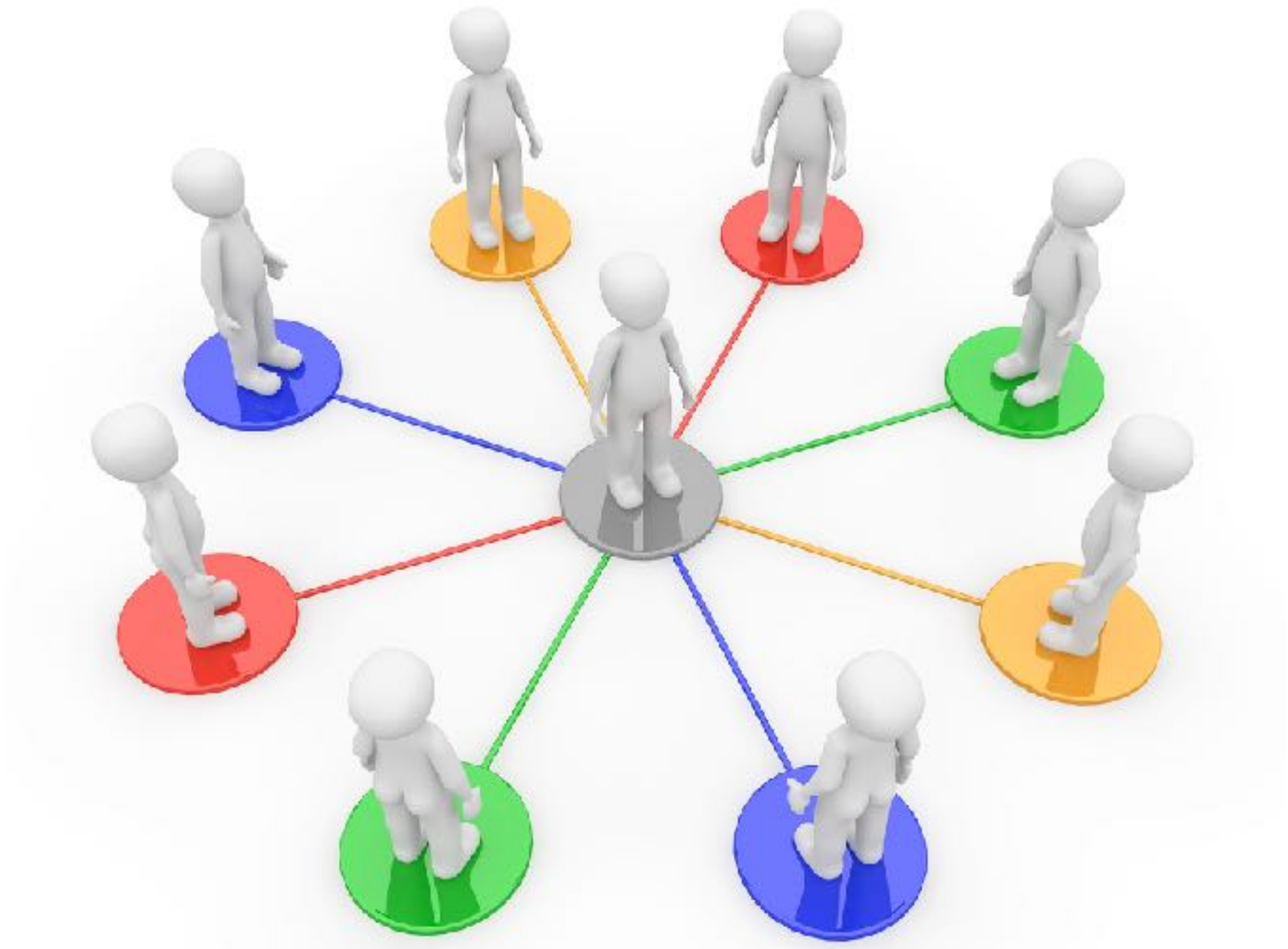
e [significato di]

“adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente”



Assenza di istruzioni

Ex art 38 GDPR titolare e responsabile devono assicurare che il DPO “non riceva alcuna istruzione per quanto riguarda l’esecuzione di tali compiti”. Il considerando 97 aggiunge che i DPO “dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in **maniera indipendente**”



indipendenza del DPO
DPO esterno vs DPO interno

DPO esterno: contratto di servizi

- La funzione di DPO può essere esercitata anche in base a un **contratto di servizi** stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che **ciascun soggetto appartenente alla persona giuridica e operante quale DPO soddisfi tutti i requisiti applicabili** come fissati nella Sezione 4 del RGPD; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi.

- Pari importanza riveste il fatto che **ciascuno dei soggetti in questione goda delle tutele previste dal RGPD:** per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto DPO, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di DPO. Al contempo, **si potranno associare le competenze e le capacità individuali** affinché il contributo collettivo fornito da più soggetti consenta di rendere alla clientela un servizio più efficiente.

- Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il team DPO, **si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del team DPO e di prevedere che sia un solo soggetto a fungere da contatto principale** e "incaricato" per ciascun cliente. Sarà utile, in via generale, **inserire specifiche disposizioni in merito nel contratto di servizi.**

indipendenza del DPO interno

Posizione del DPO:
5. “Rimozione o penalizzazioni in rapporto all’adempimento dei compiti del DPO”

Articolo 38 paragrafo 3 del Regolamento generale sulla protezione dei dati: il DPO “non è **rimosso** o **penalizzato** dal titolare del trattamento o dal responsabile del trattamento **per l’adempimento dei propri compiti**”.

Il divieto di penalizzazioni menzionato nel Regolamento generale sulla protezione dei dati si applica solo con riguardo a quelle penalizzazioni eventualmente derivanti dallo svolgimento dei compiti propri del DPO.

Per esempio, un DPO può ritenere che un determinato trattamento comporti un rischio elevato e quindi raccomandare al titolare o al responsabile di condurre una **valutazione di impatto**, ma questi ultimi non concordano con la valutazione del DPO. In casi del genere non è ammissibile che il DPO sia rimosso dall'incarico per avere formulato la raccomandazione in oggetto.

penalizzazione

DIRETTA

- mancata o ritardata promozione
- blocco delle progressioni di carriera

INDIRETTA

- mancata concessione di incentivi rispetto ad altri dipendenti.

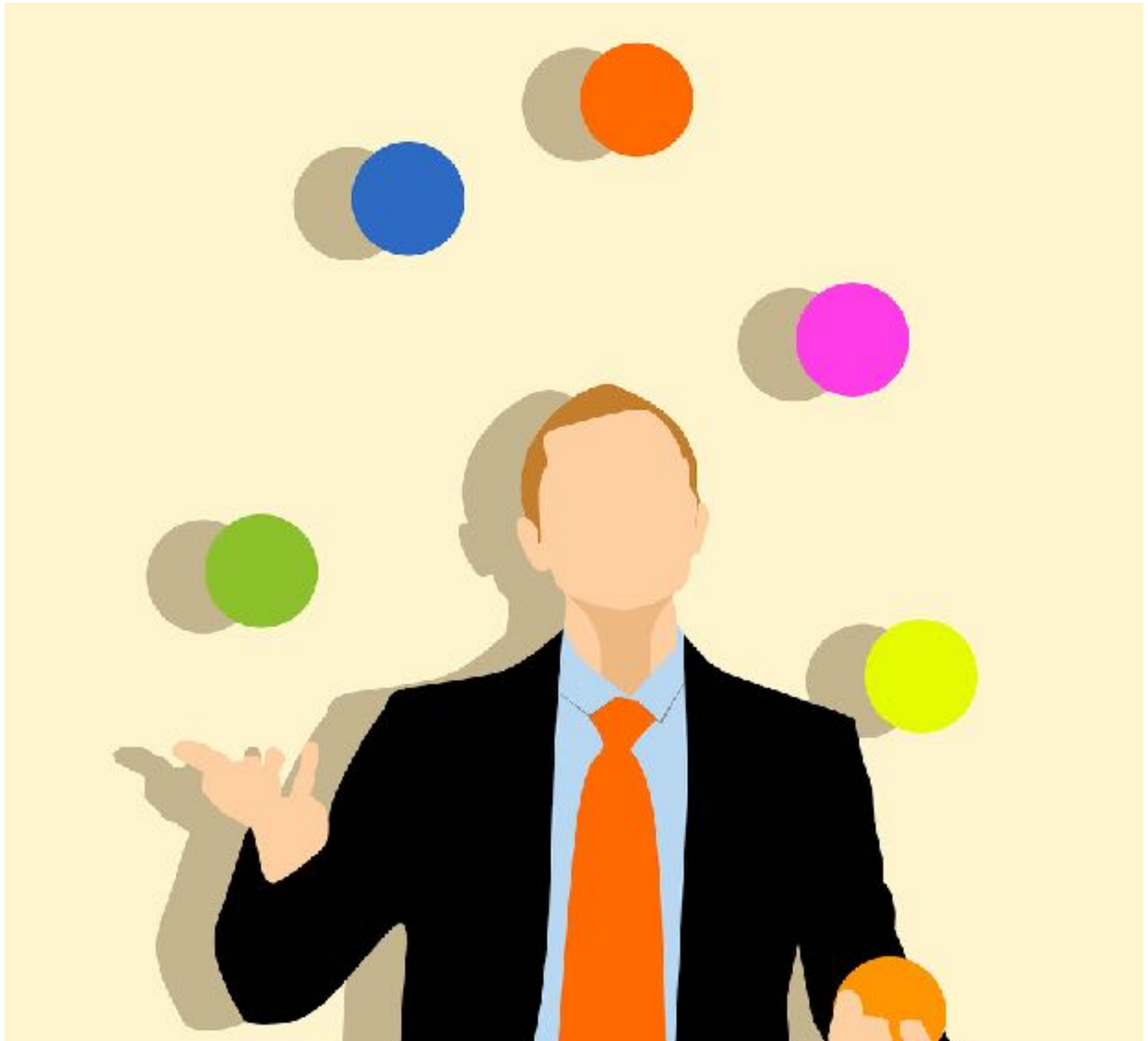
Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al DPO in rapporto alle attività da questi svolte.

è possibile interrompere il rapporto con il DPO per **motivazioni diverse dallo svolgimento dei compiti che gli sono propri**: per esempio, in caso di furto, molestie sessuali o di altro genere, o altre analoghe e gravi violazioni deontologiche.

Regole specifiche

il RGPD non specifica le modalità e la tempistica riferite alla cessazione del rapporto di lavoro del DPO o alla sua sostituzione. Tuttavia, quanto **maggiore** è la **stabilità** del contratto stipulato con il DPO e **maggiori** le **tutele** previste **contro l'ingiusto licenziamento**, tanto maggiore sarà la probabilità che l'azione del DPO si svolga in modo **indipendente**. Il WP29 vede, quindi, con favore ogni iniziativa assunta in tal senso dai titolari e responsabili di trattamento.

cosa deve fare il DPO?



Compiti del DPO:

☑ **sorvegliare l'osservanza del GDPR** (attenzione, la responsabilità per la mancata osservanza grava comunque sul titolare)**:**

1. il DPO raccoglie informazioni per individuare i **trattamenti** svolti

2. Il DPO opera l'**analisi** e la **verifica** dei trattamenti per valutarne la **conformità** al GDPR

3. il DPO svolge attività di **informazione**, **consulenza**, e **indirizzo** nei confronti del titolare e del responsabile.

Compiti del DPO:

☑ fungere da **punto di contatto per gli interessati** in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti.

☑ Cooperare con l'Autorità di controllo, fungere da **punto di contatto per l'Autorità di controllo** oppure, eventualmente, consultarla di propria iniziativa ("facilitatore").

☑ Considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo (**Approccio basato sul rischio**).

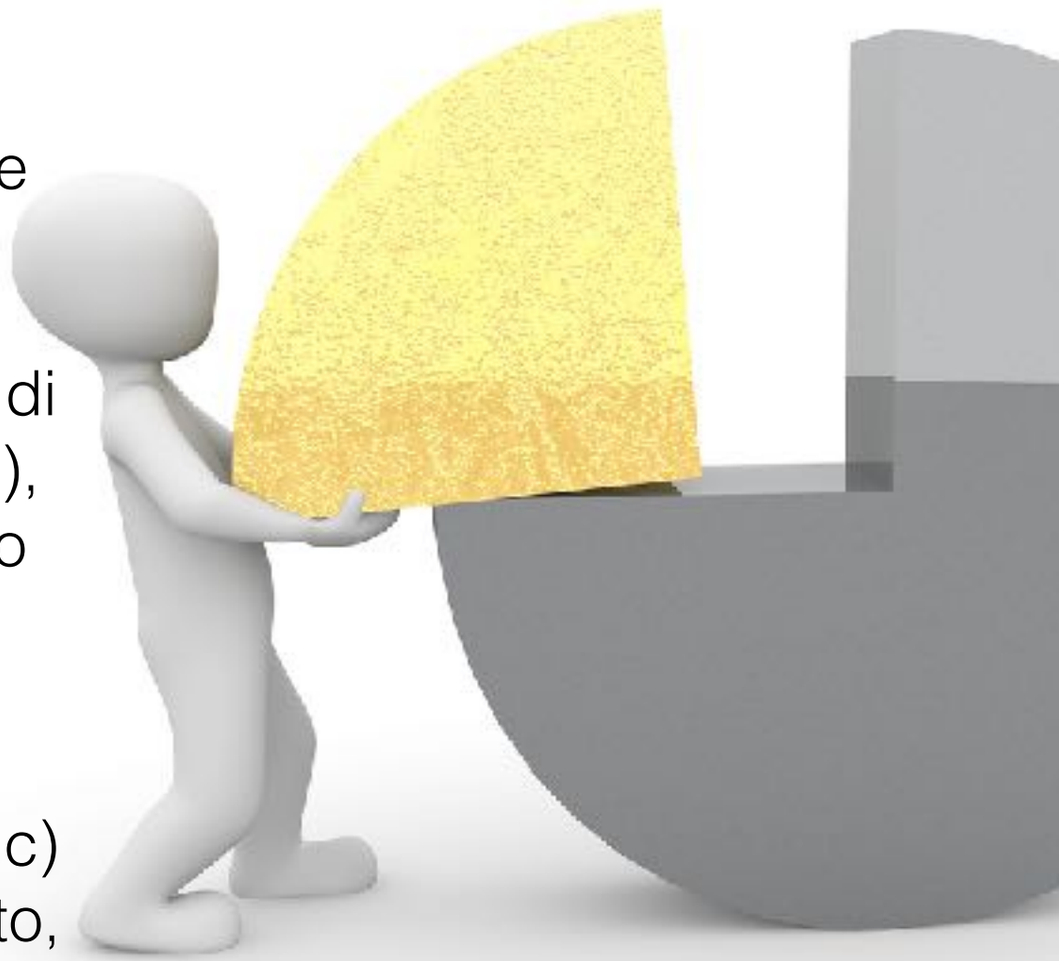
☑ Fornire, se richiesto, **pareri in merito alla valutazione d'impatto sulla protezione dei dati** e sorvegliare i relativi adempimenti;

Il ruolo del DPO nella valutazione di impatto sulla protezione dei dati

- È compito del titolare condurre la DPIA, non del DPO.

- Tuttavia, il DPO svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale DPIA. In ossequio al principio di “protezione dei dati fin dalla fase di progettazione” (o **data protection by design**), l’art. 35, secondo paragrafo, prevede in modo specifico che il titolare **“si consulta**” con il DPO quando svolge una DPIA.

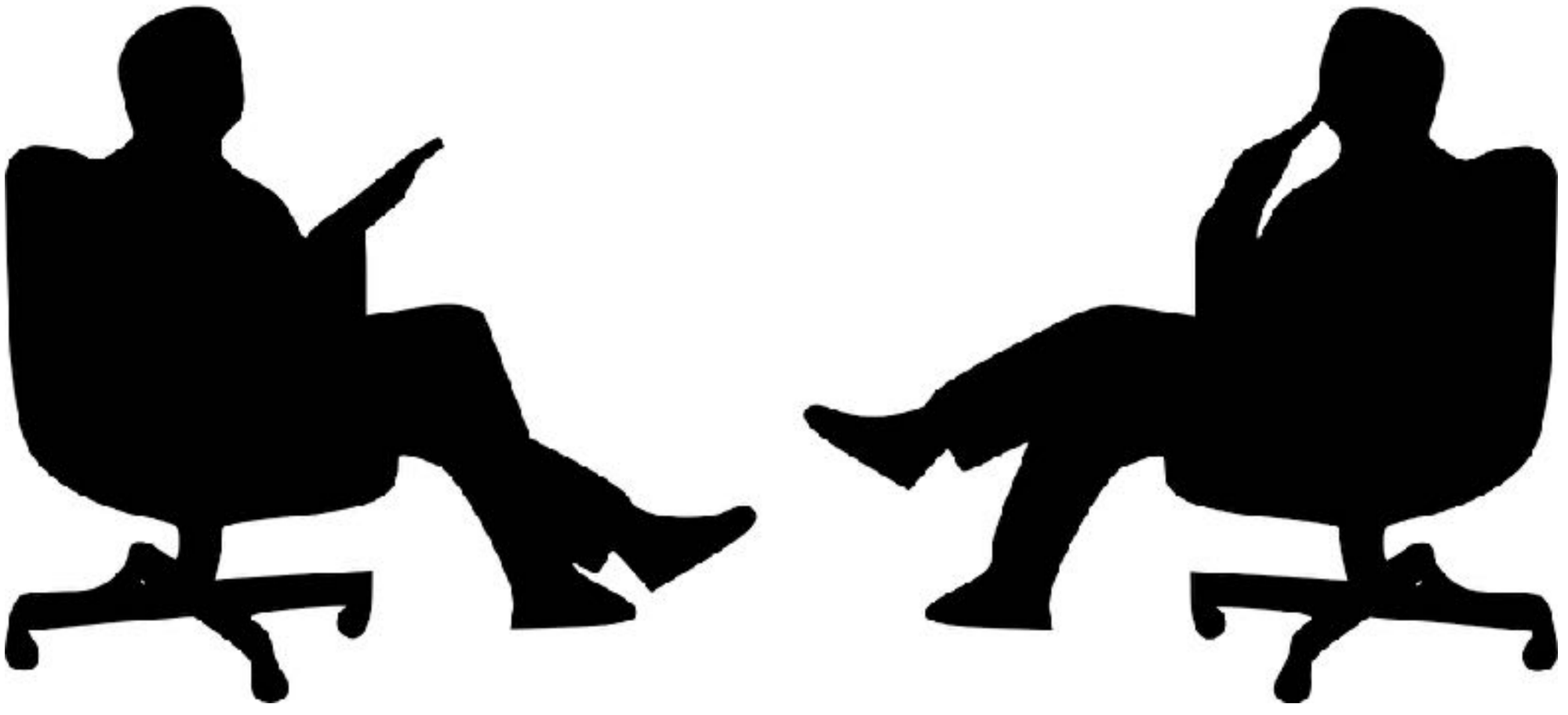
- A sua volta, l’art. 39, primo paragrafo, lettera c) affida al DPO il compito di “fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell’articolo 35”.



Il WP29 raccomanda che il titolare si consulti con il DPO, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD.

Qualora il titolare non concordi con le indicazioni fornite dal DPO, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.



il WP29 raccomanda

- che il titolare **definisca con chiarezza,** per esempio **nel contratto stipulato** con il DPO, ma anche fornendo **informative** ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa, **i compiti specificamente affidati al DPO e i rispettivi ambiti**, con particolare riguardo alla conduzione della DPIA.

Compiti del DPO:

☑ Il DPO deve anche tenere il registro delle attività di trattamento?

Buone prassi e importanza della contrattualistica

- posizione del DPO: “Ove opportuno, il titolare o il responsabile potrebbero mettere a punto **linee-guida** ovvero **programmazioni** in materia di protezione dei dati che indichino i casi di **consultazione obbligatoria** del DPO”. (pag. 14)

- **Contratto di servizi** per DPO esterno

- DPO interno: **contratto con maggiori tutele contro l'ingiusto licenziamento** (autonomia).

- **Definizione contrattuale dei compiti** attribuiti al DPO + informative

- Nel caso di team interno: **definire con precisione la struttura interna del gruppo** di lavoro nonché **i compiti** e le **responsabilità individuali**

Buone prassi in materia di conflitto di interessi

- **individuare** le qualifiche e funzioni che sarebbero **incompatibili** con quella di DPO;

- **redigere regole interne** a tale scopo onde evitare conflitti di interessi;

- **prevedere un'illustrazione più articolata** dei casi di conflitto di interessi;

Buone prassi in materia conflitto di interessi

- prevedere **specifiche garanzie** nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa di DPO ovvero nel redigere il contratto di servizi si utilizzino **formulazioni sufficientemente precise e dettagliate** così da **prevenire conflitti** di interessi. Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere **varie configurazioni** a seconda che il DPO sia designato fra soggetti **interni** o **esterni** all'organizzazione.

Grazie

Avvocato Cristina Vicarelli

www.cristina-vicarelli.it

studiolegale@cristinavicarelli.it
Twitter @cristi_vic
www.facebook.com/cri.vicarelli
it.linkedin.com/in/cristinavicarelli