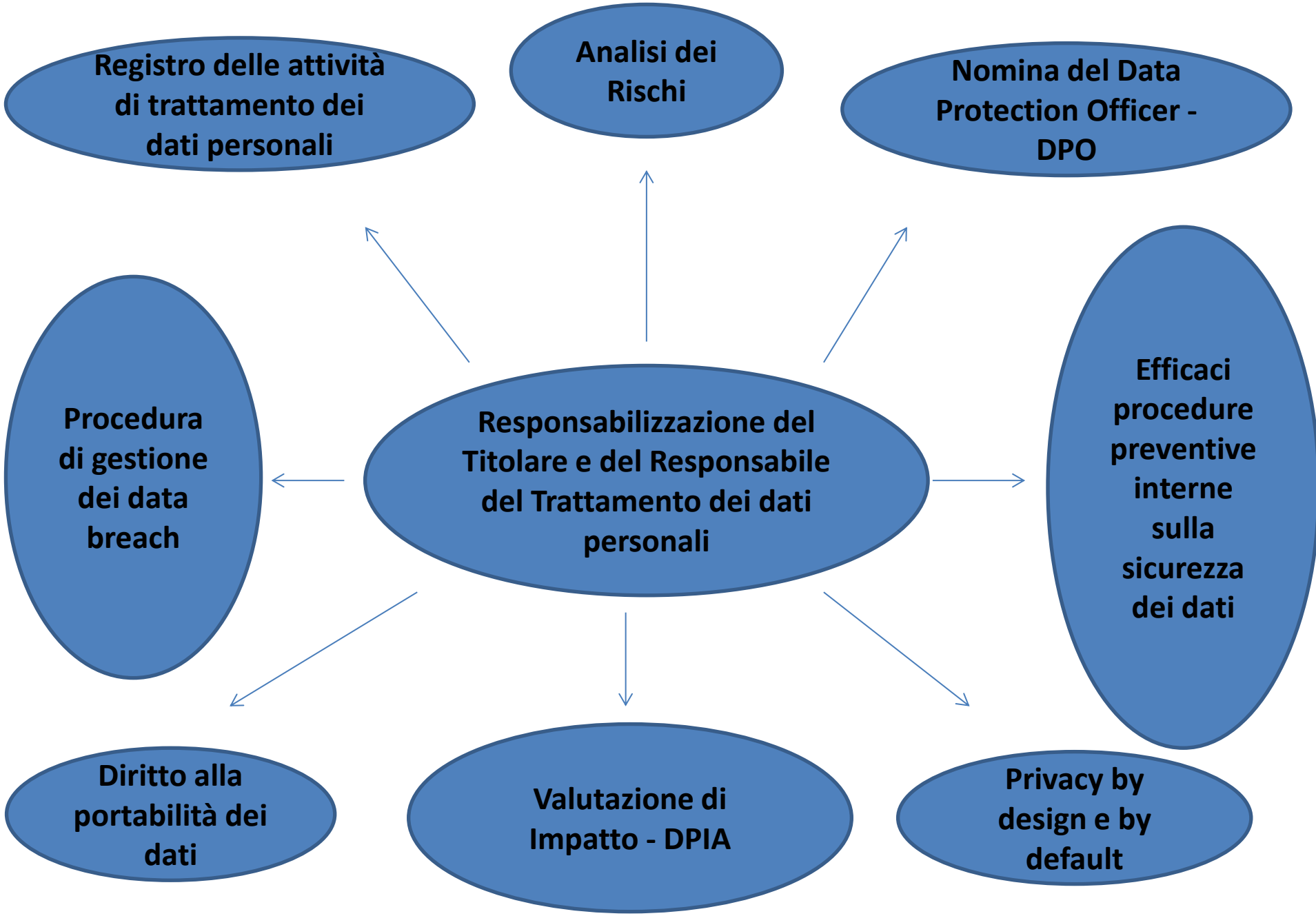
Il nuovo regolamento europeo sulla privacy - GDPR

Avvocato – Presidente del Centro europeo per la privacy – EPCE
Email: info@europeanprivacycentre.eu - www.europeanprivacycentre.eu
***Docente** a contratto Master Università «La Sapienza» di Roma – Facoltà di Economia*
***Docente** a contatto Master «Sicurezza delle reti informatiche » Università Nicolò Cusano*
LL.M. - ISO 27001 Security Lead Auditor

Relazione su:
Il ruolo del responsabile della protezione dei dati personali (Data Protection Officer): ambiti di designazione obbligatoria, analisi dei compiti e delle responsabilita'

Dal Codice della privacy agli adempimenti del Gdpr Regolamento generale per protezione dei dati personali (reg. eu 2016/679 – GDPR): un approccio al rischio proattivo sul trattamento dei dati personali


Registro delle attività di trattamento dei dati personali
Analisi dei Rischi
Nomina del Data Protection Officer - DPO
Procedura di gestione dei data breach
Responsabilizzazione del Titolare e del Responsabile del Trattamento dei dati personali
Efficaci procedure preventive interne sulla sicurezza dei dati
Diritto alla portabilità dei dati
Valutazione di Impatto - DPIA
Privacy by design e by default

Responsabile della protezione dei dati personali - Data Protection Officer

Situazione attuale in Italia prima del Regolamento EU

I soggetti coinvolti secondo il Codice della Privacy (d.lgs. 196/2003)

- Titolare del trattamento dei dati personali
- Responsabile del trattamento dei dati personali
- Incaricato del trattamento dei dati personali

Riflessione analitica sui compiti del responsabile privacy

Art. 29 del Codice della Privacy

“4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare […]

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale […] vigila sulla osservanza […] delle istruzioni ” (e il mantenimento dei requisiti soggettivi)

Riflessione analitica sul responsabile privacy

Deve:

Attenersi alle istruzioni analitiche: compiti specifici conferiti dal

titolare e non definiti dalla legge

Limiti:

- Non può agire in modo indipendente ma seguire le istruzioni
- Non è prevista una disciplina che obbliga a fornire autonomia nella gestione delle risorse economiche, di personale, altro necessario per eseguire le proprie mansioni/o il proprio servizio
- Non è prevista alcuna disciplina in ordine al conflitto di interessi che si può presentare anche con altre funzioni affidate

DPO nel quadro normativo europeo e italiano protezione dei dati personali

Data Protection Officer (DPO)

Responsabile della protezione dei dati personali

Il ruolo di Supervisore Indipendente

Interno

(rapporto di lavoro subordinato – “assunto” o “membro del personale”)

Esterno

(contratto di servizi)

DPO nel quadro normativo europeo e italiano protezione dei dati personali

Data Protection Officer (DPO)

Responsabile della protezione dei dati personali

Il ruolo di Supervisore Indipendente

Interno

(rapporto di lavoro subordinato – “dipendente” art. 37 co. 6)

Esterno

(contratto di servizi)

DPO nel quadro normativo europeo e italiano protezione dei dati personali

Data Protection Officer (DPO)

Responsabile della protezione dei dati personali

L’incarico di DPO può essere affidato a persona giuridica oppure un ente assimilabile ad essa?

Articolo 37 Designazione del responsabile della protezione dei dati

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati quando:

- **Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali**

- Le attività principali del titolare del trattamento o responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala (Si veda considerando n. 71)

- Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'art. 9 (dati sensibili inclusi i dati biometrici) o dati relativi alle condanne penali e a reati

Esclusione dai trattamenti su larga scala: medico – operatore sanitario - avvocato

Articolo 37 Designazione del responsabile della protezione dei dati

Focus autorità pubblica e organismo pubblico

le linee guida pubblicate dal Gruppo articolo 29 indicano che le nozioni di “autorità pubblica ” e di “organismo pubblico” **devono riferirsi al diritto interno dello Stato Membro**. In tal senso vanno ricompresi i Ministeri e tutti gli enti pubblici anche territoriali, ma anche tutti gli enti gestiti secondo la normativa di diritto pubblico.

Articolo 37 Designazione del responsabile della protezione dei dati

Focus autorità pubblica e organismo di diritto pubblico

Infatti, come specificato dal Gruppo art. 29 alla nota 12 per gli organismi di diritto pubblico si può fare riferimento alla **direttiva 2003/98/UE** sul riutilizzo dell'informazione nel settore pubblico (come modificata dalla direttiva 2013/37/UE), al cui art. 2 punti numero 1 e 2 è previsto che:

"Ai fini della presente direttiva si intende per:

«ente pubblico», le autorità statali, regionali o locali, gli organismi di diritto pubblico e **le associazioni formate da una o più di tali autorità** oppure da uno o più di tali organismi di diritto pubblico;

2) «**organismo di diritto pubblico**», qualsiasi organismo:

a) istituito per soddisfare specificatamente bisogni d'interesse generale aventi carattere non industriale o commerciale;

b) dotato di personalità giuridica;

c) la cui attività è finanziata **in modo maggioritario** dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico, oppure la cui **gestione è soggetta al controllo di questi ultimi**, oppure il cui organo d'amministrazione, di direzione o di vigilanza è costituito **da membri più della metà** dei quali è designata dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico".

Articolo 37 Designazione del responsabile della protezione dei dati

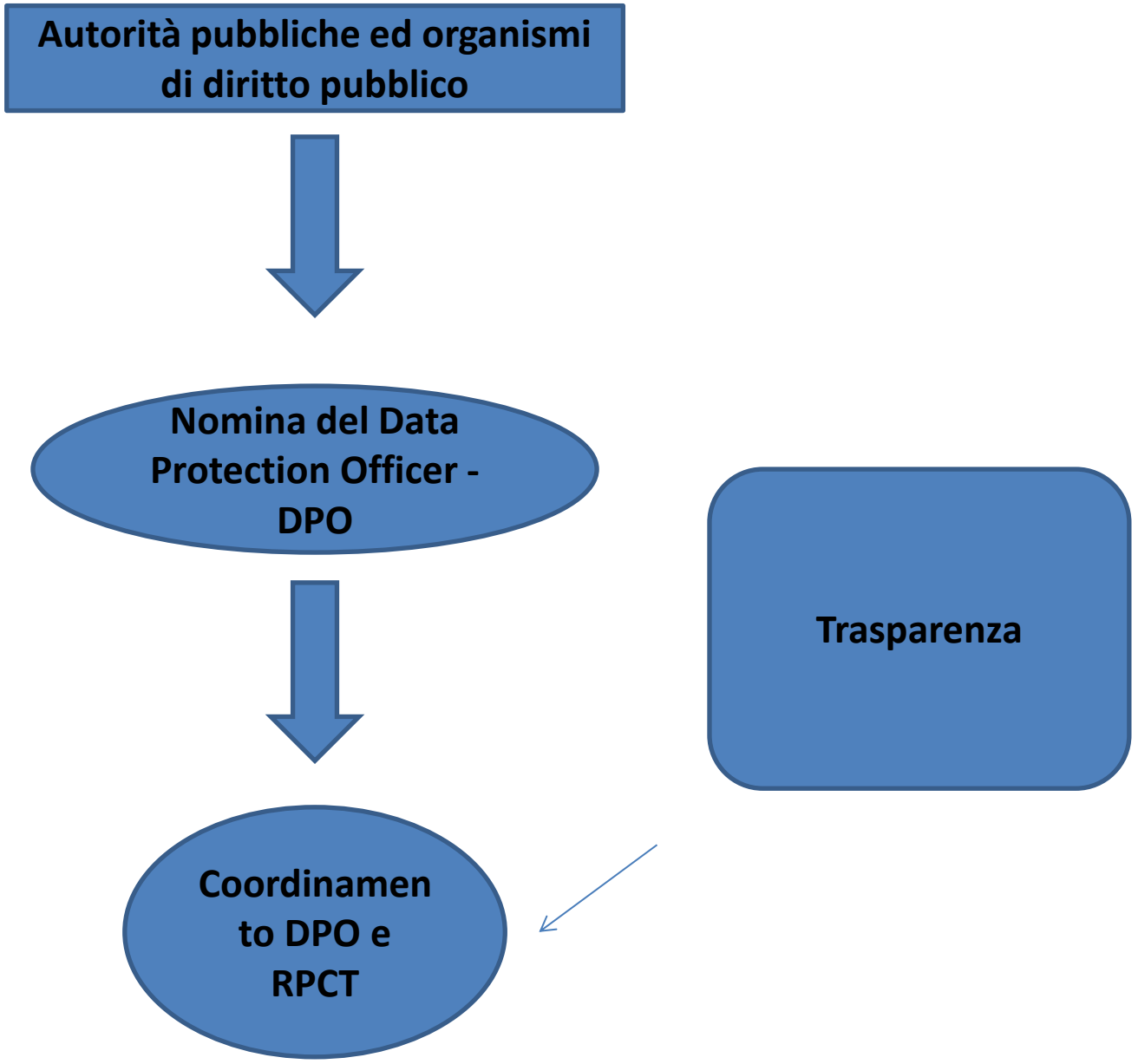
Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati quando:

- Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali

- **Le attività principali del titolare del trattamento o responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala (Si veda considerando n. 71)**

- **Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'art. 9 (dati sensibili inclusi i dati biometrici) o dati relativi alle condanne penali e a reati**

Esclusione dai trattamenti su larga scala: medico – operatore sanitario - avvocato


Autorità pubbliche ed organismi di diritto pubblico
Nomina del Data Protection Officer - DPO
Trasparenza
Coordinamento DPO e RPCT

Galassia delle attività del DPO

Elementi caratterizzanti l'indipendenza del DPO (art. 38)

Requisiti negativi

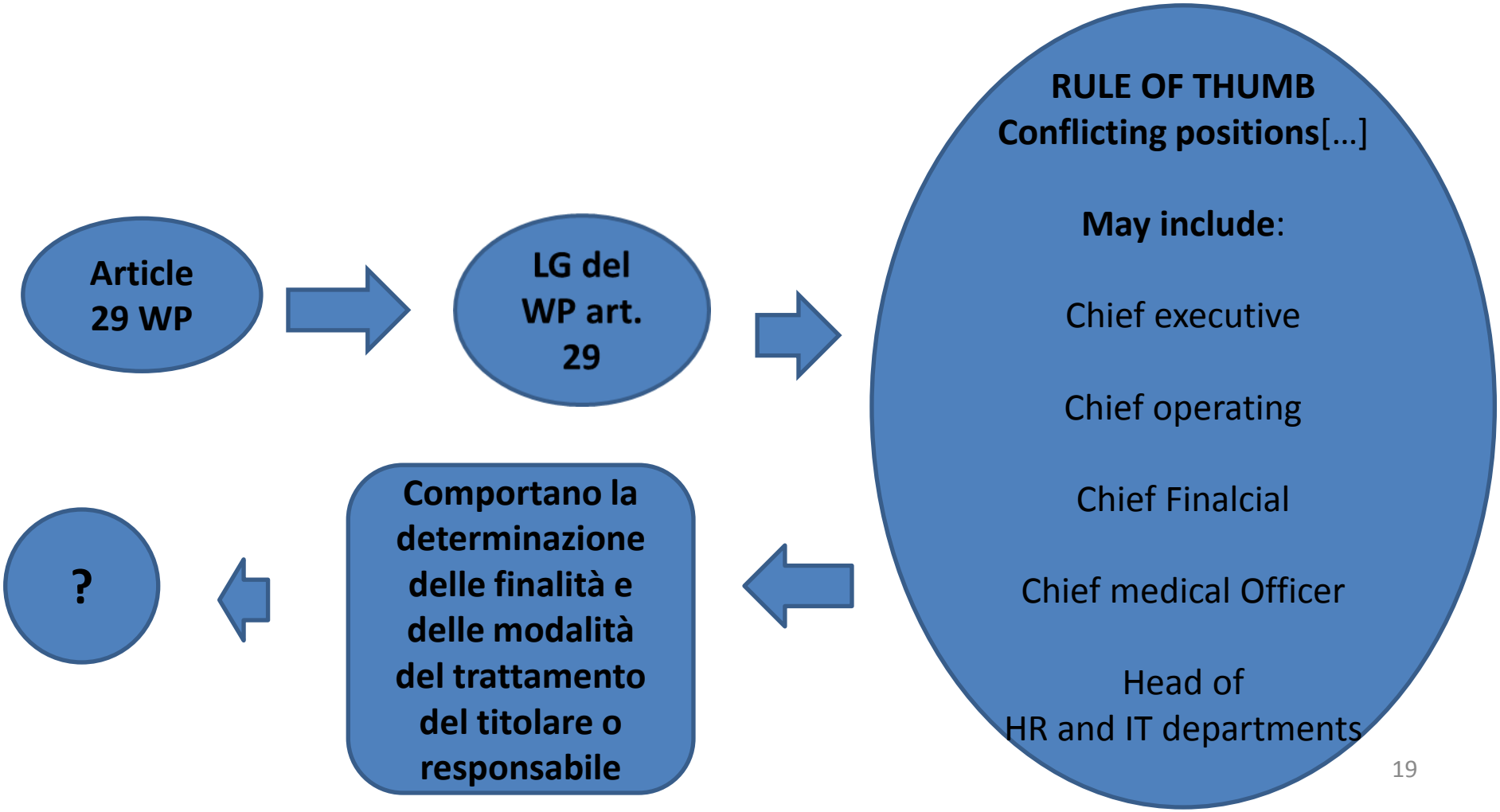
- assenza di un conflitto di interessi, *può svolgere altri compiti e funzioni*

- INDIPENDENZA: Non ingerenza nell'esercizio delle sue funzioni da parte del
- responsabile o incaricato: nessuna <<istruzione per quanto riguarda l'esecuzione dei propri compi>>
- <<non è rimosso o penalizzato[…] per l'adempimento dei propri compiti>>

***concetto di indipendenza effettiva*, nota a livello giurisprudenziale, in particolare, in ambito organizzativo come i Modelli di Organizzazione (c.d. MOGC secondo d.lgs. 231/2001) e i relativi Organismi di Vigilanza**

Elementi caratterizzanti l'indipendenza del DPO (art. 38 – Linee guida WP Art. 29)

Dubbi al DPO sono inibiti compiti operativi? IT Admintrator e DPO



Soluzioni organizzative per la designazione del DPO(art. 38)
Linee guida del Gruppo di lavoro ex art. 29
Pubblicate il 13 dicembre 2016
FAQ allegate alle Linee guida – punto 6

«se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un *team* operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente.

In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale RPD soddisfi tutti i requisiti applicabili come fissati nel RGPD.

Per favorire efficienza e correttezza, le linee-guida raccomandano di procedere a una chiara ripartizione dei compiti nel *team* del RPD esterno, attraverso il contratto di servizi, e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.»

Soluzioni organizzative per la designazione del DPO(art. 38)
Linee guida del Gruppo di lavoro ex art. 29
Pubblicate il 13 dicembre 2016
FAQ allegate alle Linee guida – punto 6

Nelle Linee guida si chiarisce pertanto che nel contratto di servizi è essenziale il requisito della personalità della prestazione professionale in base al contratto di servizi, emerge il concetto giuridico dell'*intuitus personae* e della fiducia affidata dal cliente al singolo professionista all'interno del gruppo, «un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.»

Responsabilità in termini di colpa grave, colpa lieve e dolo in capo a quest'ultimo.

Elementi per la designazione del DPO (art. 37 co. 5)
Quali sono gli standard di professionalità richiesti?
Qual è il percorso professionale?

- **conoscenza specialistica** della normativa in materia di protezione dei dati personali sulla base di trattamenti dei dati personali effettuati dal Titolare del trattamento

- **conoscenza delle prassi** in materia di protezione dei dati personali (*rectius* esperienza)

- **capacità di assolvere i compiti ex art. 39**
  (contesto, natura dei dati e complessità organizzazione)

Elementi caratterizzanti l'indipendenza e autonomia del DPO (art. 38)

Requisito positivo

«*Risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*» art. 38 co. 2 del regolamento

«vertice gerarchico del titolare del trattamento o del responsabile del trattamento»

Elementi di valutazione in base alle best pratice in ambito DPO:

Piena autonomia finanziaria per eseguire i propri compiti o richiesta ad altre funzioni interne o direttamente al Titolare del trattamento

Elementi caratterizzanti l'indipendenza e autonomia del DPO (art. 38)

<<vertice gerarchico del titolare del trattamento o del responsabile del trattamento>>

- Non deve essere pertanto parte del vertice gerarchico, ma deve riferire al Vertice gerarchico, si esclude in linea generale che il DPO debba essere:

- Un consigliere di un CDA del titolare o del responsabile del trattamento che lo designa tale, tenuto conto del conflitto di interessi e dell'indipendenza come elemento necessario.

Il DPO interno dovrebbe avere sufficiente tempo per svolgere i propri compiti, eventuali assunzioni a part- time dovrebbero essere quindi valutati con particolare attenzione e cum grano salis

Una figura junior potrebbe avere troppo poca esperienza per gestire relazioni con il vertice e mantenere al contempo una propria indipendenza

Aspetti pratici sul DPO

Prime osservazioni pratiche

L'organizzazione prima di procede alla gara di appalto o alla designazione interna dovrà provvedere a:

«- individuare le qualifiche e funzioni che sarebbero incompatibili con quella di RPD;
- redigere regole interne a tale scopo onde evitare conflitti di interessi;
- prevedere un'illustrazione più articolata dei casi di conflitto di interessi;
- dichiarare che il RPD non versa in alcuna situazione di conflitto di interessi con riguardo alle funzioni di RPD, al fine di sensibilizzare rispetto al requisito in questione; […]»

Aspetti pratici sul DPO

Prime osservazioni pratiche

L'organizzazione per prima di procede alla gara di appalto o alla designazione interna dovrà provvedere a:

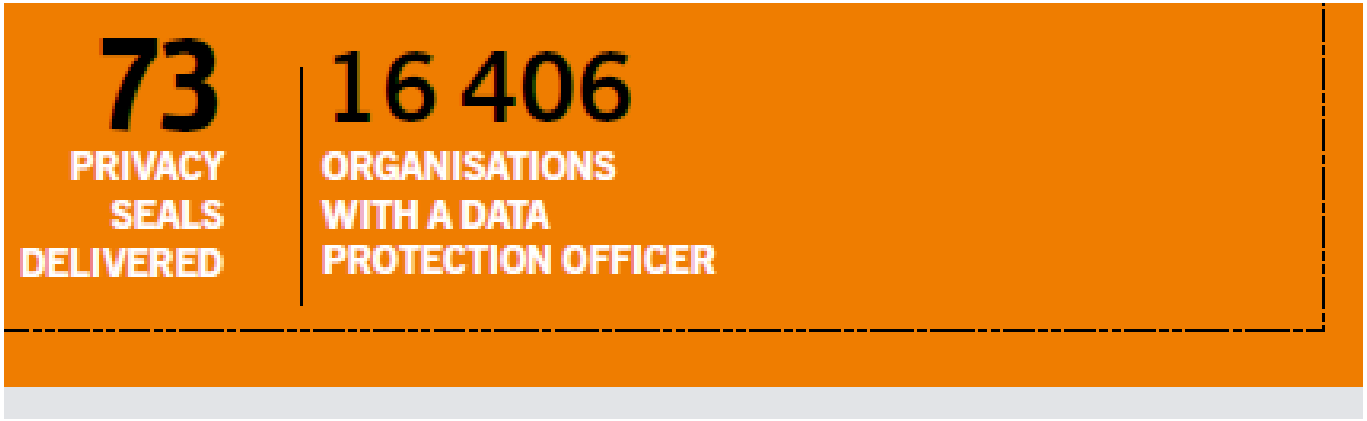
«- prevedere specifiche garanzie nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa quale RPD ovvero nel redigere il contratto di servizi si utilizzino formulazioni sufficientemente precise e dettagliate così da **prevenire conflitti di interessi**. Al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

L'organizzazione deve quindi dotarsi di Codici etici, politiche e procedure volte a garantire che l'RPD operi in contesto legale-organizzativo che gli consenta di rispettare la normativa vigente

Aspetti pratici sul DPO

L'opportunità del nuovo ruolo del DPO

Il Cnil – Autorità Garante privacy francese ha pubblicato un report riferito all'anno 2015 nel quale specifica che nonostante sia prevista nella normativa nazionale francese solo una designazione facoltativa vi erano fino al 2015 già oltre 16.000 organizzazioni che avevano scelto di dotarsi di tale figura



Link utili di approfondimento sul RPD/DPO

http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-09-26/dpo-data-protection-officer-responsabile-protezione-dati-personali-174216.php - **DPO – Data Protection Officer: il responsabile della protezione dei dati personali - CRISTIANO COMINOTTO – ANNA MINICHIELLO – FRANCESCO CURTARELLI – 20 giugno 2016**

http://www.agendadigitale.eu/infrastrutture/data-protection-officer-si-chiariscono-le-novita-del-regolamento-privacy-europeo_2844.htm - **Data protection officer, si chiariscono le novità del Regolamento privacy europeo – GABRIELE FAGGIOLI – 23 gennaio 2017**

http://www.corrierecomunicazioni.it/ict-law/45112_data-protection-officer-troppi-problemi-interpretativi-serve-piu-chiarezza.htm -

Data protection officer: troppi problemi interpretativi, fare chiarezza – FABIO DI RESTA – 27 dicembre 2016

http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2016-12-21/il-ruolo-data-protection-officer-anche-italia-e-obbligatorio-la-pubblica-amministrazione-e-ambito-privato-pubblicate-linee-guida-gruppo-europeo-garanti-privacy-121040.php
Il ruolo del Data Protection Officer anche in Italia è obbligatorio per la pubblica amministrazione e in ambito privato: pubblicate le linee guida del Gruppo europeo dei Garanti privacy – FABIO DI RESTA – 21 dicembre 2016

http://www.agendadigitale.eu/infrastrutture/norme-privacy-ue-ecco-tutto-cio-che-bisogna-sapere-su-accountability-e-sicurezza_2279.htm - **Norme privacy UE, ecco tutto ciò che bisogna sapere su accountability e sicurezza – MAURO ALOVISIO E FABIO DI RESTA – 20 giugno 2016**

https://www.youtube.com/watch?v=sMpveaZKZ2A – **Compiti e responsabilità del "data protection officer - FABIO DI RESTA – 26 dicembre 2016**

http://www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili - Giuda all'applicazione del GDPR pubblicata sul sito del Garante il 28 aprile 2017

Grazie per l'attenzione

Avvocato – Presidente del Centro europeo per la privacy – EPCE
Email: info@europeanprivacycentre.eu - www.europeanprivacycentre.eu
***Docente** a contratto Master Università «La Sapienza» di Roma – Facoltà di Economia*
***Docente** a contatto Master «Sicurezza delle reti informatiche » Università Nicolò Cusano*
LL.M. - ISO 27001 Security Lead Auditor