- **Potete circoscrivere il contenuto della delega che il dirigente può adottare come responsabile interno?**

Il Responsabile interno può delegare a un proprio Referente strutturato, docente o tecnico amministrativo, i compiti a lui assegnati (e dettagliati nell'atto di nomina), relativamente ai diversi ambiti di competenza. La delega è formalizzata con apposito atto, contiene puntualmente i compiti delegati ed è corredato dalle relative istruzioni e dalle individuazione delle modalità di verifica e di controllo. Di tale delega è data comunicazione a Titolare e RPD, viene data adeguata evidenza nel registro dei trattamenti e ampia diffusione all'interno dell'amministrazione universitaria e attraverso gli strumenti di partecipazione esterna.

- **Nel caso di piccoli Atenei senza Dirigenti il modello organizzativo prevede il conferimento agli EP del ruolo di Responsabili interni?**

Nel caso di piccoli Atenei come anche in atenei di dimensioni maggiori, si ritiene che il ruolo di responsabile interno possa essere conferito agli EP o di categoria D come anche a personale docente. In ogni caso il Titolare potrebbe procedere direttamente a designare gli autorizzati fornendo loro le relative istruzioni (come previsto dall'art. 29 del GDPR)

- **Solo agli EP?**

Non solo a EP, ma è comunque preferibile che i responsabili siano titolari di posizioni organizzative apicali.

- **E' possibile conoscere le motivazioni della scelta di nominare responsabili interni (ex art. 28 GDPR) e non designati (ex d.lgs 101/2018)?**
- **Il ruolo di Responsabile Interno è molto discusso in quanto tale a livello di GDPR; il Garante ha espresso parere positivo su tale specifica previsione regolamentare ? Grazie**
- **Il Responsabile del Trattamento è un Data Processor, non un Data Controller, cioè non è un subresponsabile del Titolare (Ateneo che si fa rappresentare dal Rettore, con un organigramma privacy interno). Per questo chiedevo se il Garante si fosse espresso in proposito: tra Codice pre GDPR e GDPR c'è stato un salto qualitativo colto nella versione originale in inglese, non nel testo italiano, e questo potrebbe creare problemi. Grazie comunque per le indicazioni, naturalmente**
- **E' fondamentale conoscere le motivazioni di questa scelta (responsabili interni) e sapere se il Garante ha espresso parere in merito. E' quasi unanime l'orientamento che vede l'art. 28 GDPR riferito solo a responsabili esterni. Una scelta diversa va motivata**
- **Il gdpr sembra prevedere la nomina a responsabile del trattamento solo in capo a soggetti esterni (es. fornitori) all'organizzazione dell'ente. La nomina di responsabili interni non crea problematiche a livello di applicazione della norma anche in termini di responsabilità su persone fisiche nominate a responsabili? non è più corretto parlare di incaricati interni?**
- **Il Responsabile ex art. 28 deve anche "presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative ..."**
- **Da quel che mi risulta (spero di non ricordare male) in sede di elaborazione delle linee guida Codau, il Garante si era già espresso in merito al quesito del responsabile ex art. 28 GDPR (interno e/o esterno?) confermando che è da intendersi SOLO ESTERNO e**

**che eventuali figure interne di supporto vanno definite terminologicamente in modo differente. Anche pechè sono figure anche sostanzialmente differenti sotto vari profili, non ultimo quello della responsabilità... Spero in un chiarimento da parte della CRUI. Grazie.**

- **Anche noi a Palermo ci stavamo orientando per individuare referenti/delegati interni del Titolare senza alcuna responsabilità salvo che nella nomina degli autorizzati e della vigilanza**

**I responsabili interni come indicati nella bozza di regolamento non corrispondono alla figura del responsabile ex art. 28 del GDPR** (indicati come responsabili esterni nella bozza di regolamento) bensì al **soggetto designato** ex art. 2-quaterdecies D.Lgs. 196/2003 come novellato dal D.Lgs./2018. L'articolo in questione - rubricato *Art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati)* – indica al comma 1 che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilita' e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali* siano *attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità".*
La **scelta lessicale** di indicare tali soggetti come **responsabili interni** rientra nell'ambito di scelte interne in relazione al modello organizzativo adottato. La delega di alcuni compiti da parte del titolare si configura, in questo caso, come uno strumento normale di organizzazione.
I **responsabili interni** sono individuati sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono.

Inoltre l'eventuale carenza di misure organizzative (e in questo può rientrare l'omessa individuazione e responsabilizzazione di soggetti interni in riferimento al trattamento e alla protezione dei dati personali) può configurarsi come violazione del principio di responsabilizzazione (art. 5, paragrafo 2 del GDPR) e dare luogo a responsabilità.
Infatti il Titolare, come specificato dall'art. 24 e dai Considerando 74-78 del GDPR, oltre a mettere in atto misure adeguate ed efficaci, deve essere in grado di dimostrarne l'efficacia. Tali misure, inoltre, "dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento…"

In vari incontri il Garante ha ribadito che i responsabili come individuati dall'art. 28 del GDPR possono essere solo esterni e che i rapporti con il titolare devono essere disciplinati necessariamente da un contratto o da altro atto giuridico (art. 28 GDPR). Ciò resta indiscusso. Ma il Regolamento non vieta di utilizzare il termine di responsabile interno per denominare alcune figure nella filiera organizzativa di amministrazioni complesse. L'importante è definire bene i compiti delegati e vigilare sull'espletamento di tali compiti.

E' importante non confondere la figura degli autorizzati (ex incaricati) con i responsabili interni. Gli autorizzati, comma 2 dell' art. 2-quaterdecies D.Lgs. 196/2003, sono i soggetti che trattano materialmente i dati e che sono istruiti in tal senso dal titolare.

- **Il dirigente può delegare in toto ad altri?**

Trattasi di scelte organizzative, ma è sconsigliabile delegare in toto. La scelta di concedere la possibilità di delegare alcuni compiti per particolari ambiti deriva dalla eterogeneità degli ambiti di trattamento in essere nelle università e dalla consapevolezza che vi possano essere per ciascun ambito più soggetti che per esperienza, capacità e affidabilità possano garantire il pieno rispetto e l'esecuzione dei compiti assegnati e delle istruzioni impartite dal Titolare.

- **Come deve essere individuato il soggetto autorizzato a conferire la nomina a responsabile esterno nell'ambito di un contratto ?**

Dipende dall'organizzazione interna agli Atenei. Certamente può essere uno dei compiti assegnati ai responsabili interni, ciascuno per le proprie competenze, ove si tratti di dirigenti e/o direttori di dipartimento, già giuridicamente autorizzati a firmare contratti o atti giuridici. Possono anche essere previste selezioni interne o altri modelli di scelta.

- **Sul trasferimento di dati verso Paesi extra UE la CRUI ha in programmo di redigere un codice di condotta ai sensi dell'art. 40 GDPR?**

Come riferito nel corso del webinar, oltre alle regole di attrazione alla disciplina europea e interna di dati extra UE, sembra opportuno definire anche con paesi terzi anche regole di condotta.
La CRUI interloquirà con il Garante in merito come anche nell'ambito dell'EUA o in altri organismi internazionali.

- **Che ruolo ha il responsabile della transizione al digitale?**

I compiti del responsabile della transizione al digitale sono ben specificati nella Circolare n. 3, adottata dal Ministro Bongiorno (http://www.funzionepubblica.gov.it/articolo/dipartimento/01-10-2018/circolare-n3-del-2018)

- **Come devono essere trattati i dati di connessione alla rete dell'ateneo degli utenti? Per quanto devono essere conservati i dati di connessione? Si devono quanto si deve minimizzare i dati di connessione? Inoltre, se un utente richiede la cancellazione dei propri dati di connessione, siamo costretti a farlo oppure possiamo rapportare la problematica alla normativa dei service provider che prevedono la conservazione dei dati di connessione per una durata minima di 1 anno a un massimo di 5 anni?**
- **Sarebbe utile un modello di "scheda di progetto di ricerca" conforme alle prescrizioni del Regolamento Deontologico. Si potrebbe prevedere?**
- **Mi associo all'auspicio in merito ad una scheda di progetto o linee guida CRUI conseguenti al Codice deontologico del Garante sulla ricerca. Grazie**

Tali temi costituiscono oggetto di approfondimento specialistico. A tale fine la CRUI ha avviato una importante interlocuzione sia con il Garante che con AGID . Sarebbe utile la costituzione di gruppi di lavoro anche con il CODAU.

- **Al corso organizzato per marzo sarebbe molto utile fare un focus sul trasferimento dati extra UE e sul trattamento dati automatizzato. Inoltre sarebbe utile coinvolgere anche i nostri responsabili IT con una parte sulla sicurezza infomatica e sulla "ragionevolezza dei mezzi" usati per raccogliere e conservare i dati di cui parlava il Prof. Uricchio**

Ringrazio per la sollecitazione che provvedo a girare ai docenti tecnici che interverranno al corso di marzo .

- **In caso di affidamento servizi ad aziende multinazionali il fornitore spesso rimanda alle loro privacy policy e non ritiene di condividere un atto giuridico questa modalità operativa possiamo considerarla adeguata al dettato del GDPR?**

Occorre un approfondimento delle regole adottate che dovranno essere comunque partecipate al committente anche al fine di verificare se sono aderenti alla prescrizione del regolamento europeo e alle norme interne statuali e regolamentari adottate.
Ove necessario, è sempre possibile richiedere un parere al Garante.

**Mi associo al suggerimento di far partecipare al dibattito anche i responsabili della sicurezza informatica che devono assicurare l'analisi degli incidenti di sicurezza utilizzando i dati traffico internet e attacchi alla posta elettronica.**

Suggerimento assolutamente condivisibile.