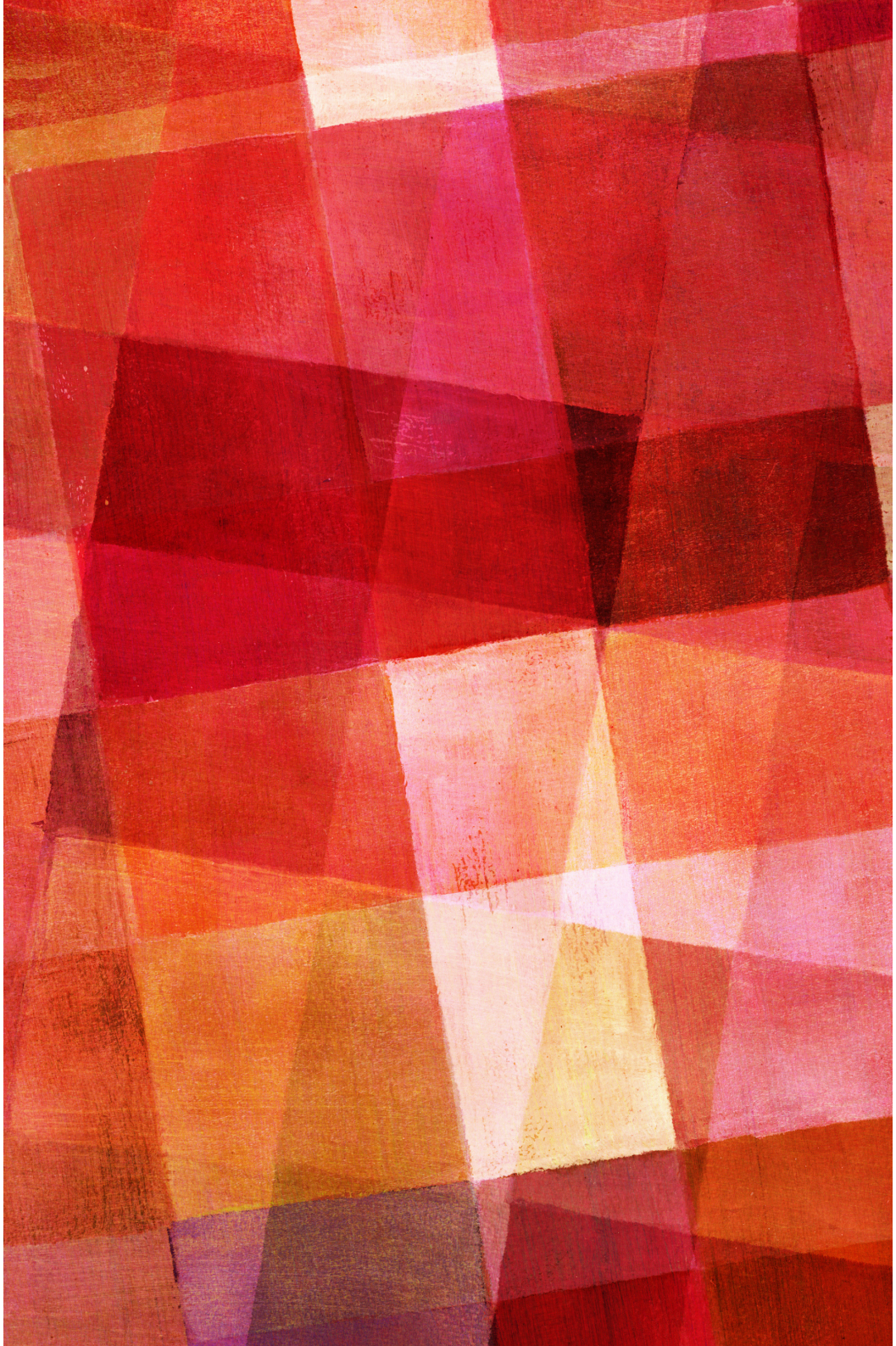


GARR 2018
DATA-REVOLUTION

Governance dei dati e conformità in materia di privacy. GDPR ricerca scientifica e *data ownership*

Dr. Nadina Foggetti
University of Bari A. Moro - Department of Law





INDICE

- GDPR e ricerca scientifica
- Data lake e trattamento dei big data: una possibile “terza via”
- DPO e ricerca scientifica ultime novità dalla giurisprudenza amministrativa

GDPR E RICERCA SCIENTIFICA

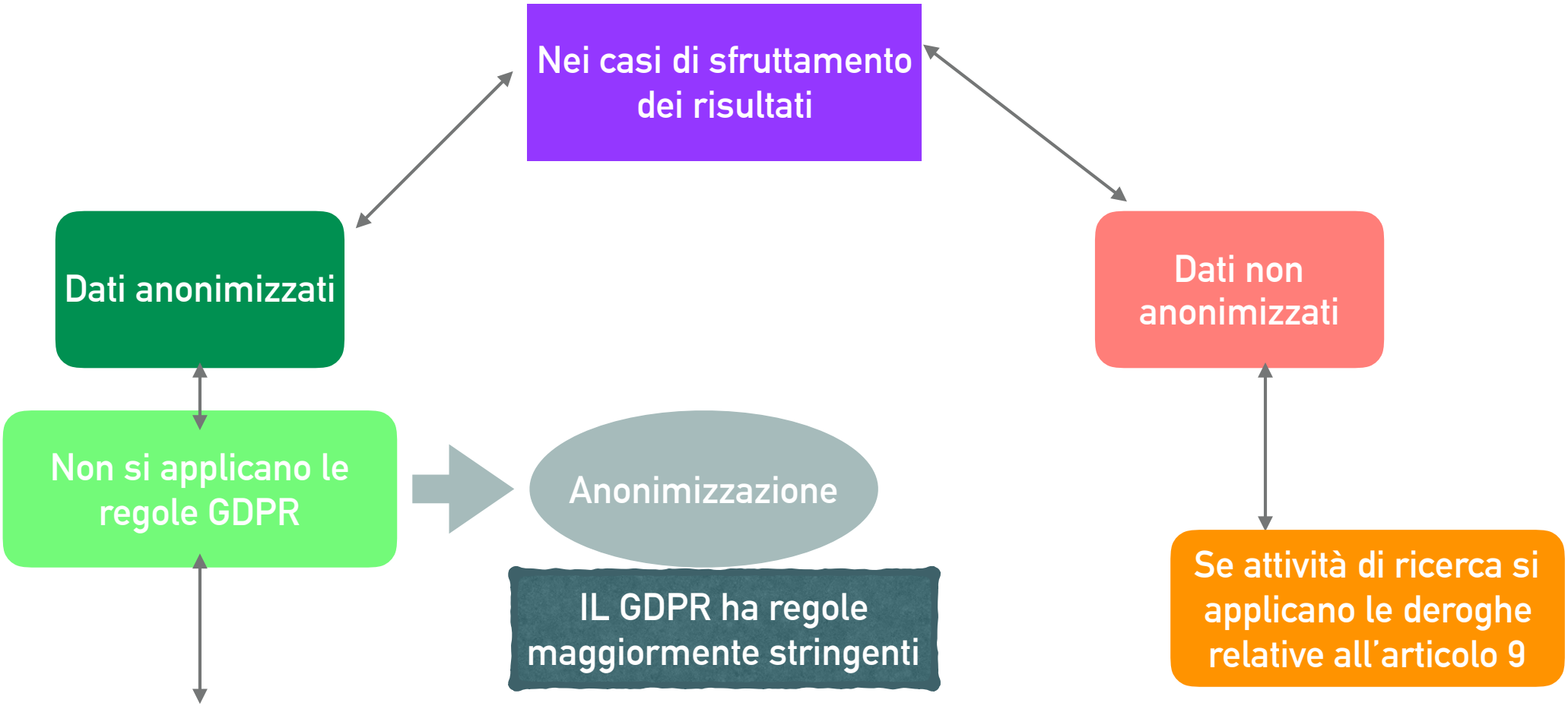
- Cosa si intende per ricerca scientifica?
  - Considerando 159 GDPR:
  - il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere:
    - sviluppo tecnologico e dimostrazione, ricerca fondamentale, **ricerca applicata e ricerca finanziata da privati**, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE
    - studi svolti nell'interesse pubblico nel settore della sanità pubblica.

- Ed effettua espressamente un riferimento all'uso aperto dei data set, nel rispetto del principio di libera circolazione dei dati che informa di se l'intero Regolamento *"dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica. Se il risultato della ricerca scientifica, in particolare nel contesto sanitario, costituisce motivo per ulteriori misure nell'interesse dell'interessato, le norme generali del presente regolamento dovrebbero applicarsi in vista di tali misure"*.
- Definizione sulla base di dati soggettivi ma oggettivi e introduce un principio di funzionalità nel trattamento, necessità del trattamento e proporzionalità (art. 9 GDPR).
- "universal access to all bona fide analytical users" - Codice di Condotta

REGOLAMENTO EUROPEO N.1290 DEL 2013

- Oggetto: “condivisione dei risultati della ricerca”.
- La **comunicazione** dei risultati della ricerca è volta dimostrare alla società e in particolare a specifici gruppi di destinatari come i fondi europei contribuiscano ad affrontare certe sfide per la società attraverso il finanziamento della ricerca
- **dissemination o diffusione dei risultati** della ricerca è una attività complessa e più tecnica (accedere e usare i dati raccolti)
- **trasferimento tecnologico (cd. exploitation)**, al fine di consentire uno sfruttamento economico della conoscenza sviluppata attraverso la ricerca **Data Sharing Policy** prevista per i Progetti H2020.

SFRUTTAMENTO ECONOMICO DEI RISULTATI DELLA RICERCA



L'ente destinatario dei dataset dovrà adottare misure organizzative volte a tenere ben distinte le attività di ricerca da quelle volte alla realizzazione di prodotti commerciali, e conseguentemente tenere anche i dataset "fisicamente" distinti, per fare in modo che il regime agevolato si applichi limitatamente ai trattamenti effettivamente svolti per scopo di ricerca.

IL DECRETO LEGISLATIVO N. 101/2018 PUBBLICATO IN GU DEL 19 SETTEMBRE 2018

- Introduce delle norme specifiche che modificano ed innovano gli aspetti relativi all'uso dei dati in materia di ricerca scientifica.
- Principi di necessità, proporzionalità e funzionalità cristallizza la **golden rule** della non necessità del consenso nelle ipotesi di ricerca medica, biomedica ed epidemiologica, qualora sia rispettato quanto disposto dall'articolo 9, par. 2, lettera j del Regolamento (art. 110 del Decreto legislativo)..
- ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria se ricorrono due circostanze:
  - previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed e' condotta e
  - resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.(p**rincipio di autonomia nel trattamento e accountability**).
  - Il consenso non è necessario quando viola il principio di proporzionalità (risulta impossibile o implica uno sforzo **sproporzionato**) e **funzionalità** (*rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalita' della ricerca)*
- In tali casi, il titolare del trattamento
  - adotta misure appropriate per tutelare i diritti, le libertà' e i legittimi interessi dell'interessato,
  - il programma di ricerca e' oggetto di motivato parere favorevole del competente comitato etico a livello territoriale
  - deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.
  - In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del regolamento nei riguardi dei trattamenti di cui al comma 1, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.»;

AI SENSI DELL'ARTICOLO 110 BIS DEL DECRETO LEGISLATIVO

- Il Garante può autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 del Regolamento, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività quando:
  - a causa di particolari ragioni, informare gli interessati risulta impossibile
  - o implica uno sforzo sproporzionato,
  - oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca,
  - a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 del Regolamento, comprese forme preventive di **minimizzazione e di anonimizzazione dei dati.**
  - Data **minimization** e **anonimizzazione**

ANONIMIZZAZIONE E PSEUDOANONIMIZZAZIONE

- GDPR estende il concetto di dati personali- identificabilità mediante incrocio di informazioni
- La Corte di Giustizia europea ha espressamente definito l'indirizzo IP (Internet Protocol) come dato personale, anche con riferimento all'IP dinamico (sentenza Breyer contro Germania del 2016)
- Il nuovo Regolamento europeo in materia di tutela dei dati personali (General Data Protection Regulation) include espressamente nei dati personali gli identificatori online, quali numeri IP, cookie e dati di geolocalizzazione.
- La Convenzione 108 e il regolamento europeo prevedono che i dati devono essere conservati per un periodo di tempo limitato, e in particolare non oltre il tempo necessario per raggiungere lo scopo alla base del trattamento. Nel caso in cui un titolare del trattamento volesse mantenerli per un periodo superiore, deve procedere alla loro anonimizzazione.
  - **Dati anonimizzati** sono quei dati che sono stati privati di tutti gli elementi identificativi. I dati anonimizzati non sono ritenuti dati personali, e quindi non sono soggetti alle norme a tutela dei dati personali.
  - **Dati pseudonimi** sono quei dati personali nei quali gli elementi identificativi sono stati sostituiti da elementi diversi, quali stringhe di caratteri o numeri (*hash*), oppure sostituendo al nome un nickname, purché sia tale da rendere estremamente difficoltosa l'identificazione dell'interessato. Ovviamente il soggetto che detiene la chiave per decifrare i dati (cioè collegare l'elemento pseudonimo al dato personale) deve garantire adeguate misure contro possibili abusi. I dati pseudonimi, a differenza di quelli anonimizzati, sono comunque dati personali

TRA ANONIMIZZAZIONE E PSEUDOANONIMIZZAZIONE

- L'art.11 e il considerando 57: L'impatto sull'analisi dei dati a fini di ricerca scientifica:
  - "se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato ai soli fini di rispettare il regolamento".
  - "qualora nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione".
- Considerando 57:
  - "Se i dati che tratta non gli consentono di identificare una persona fisica, il **titolare del trattamento non dovrebbe esser obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una norma del regolamento**. Tuttavia il titolare del trattamento **non dovrebbe rifiutare le ulteriori informazioni fornite dall'interessato al fine di sostenere l'esercizio dei suoi diritti**.
  - L'identificazione digitale di un interessato, ad esempio mediante un meccanismo di autenticazione quali le stesse credenziali utilizzate dall'interessato per l'accesso (log in) al servizio on line offerto dal titolare del trattamento.

EFFETTI

- Obiettivo dell'articolo 11 è consentire al titolare di adottare, in ragione delle finalità perseguite, modalità di trattamento di dati "deindicizzati" o comunque privi di modalità di identificazione delle persone, anche se questo comporta la privazione della possibilità di esercitare i loro diritti.
- Ai sensi del Considerando 57, un titolare acquisisce dati che sono personali perché riferibili a persone identificate o identificabili, ma non ha interesse a raccogliere ed utilizzare anche gli elementi che possono consentire tale identificazione, in quanto **inutili** ai fini dei trattamenti che vuole porre in essere.
- Il Considerando 57 estende l'efficacia dell'articolo 11.
- Non si tratta di un'anonimizzazione : costosa e contestabile
- Non si tratta di una pseudoanonimizzazione: che richiede specifiche tutele rispetto all'interessato.
- consente ai titolari di porre in essere attività di Big Data e Data Analysis utilizzando dati strutturalmente personali ma che, o perché raccolti senza identificativi o perché trattati cancellando ogni indicatore relativo a persone, possono consentire trattamenti di norma non sottoposti ad una rigida tutela degli interessati.

DPO

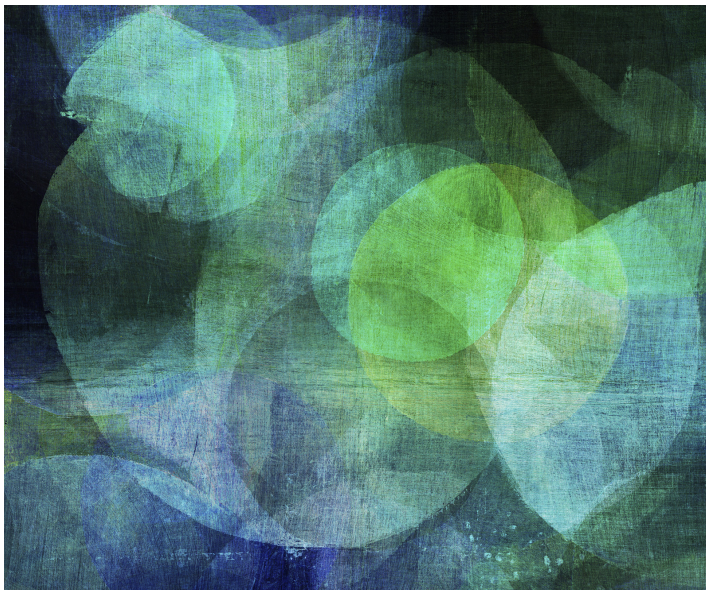
- Quando: Art. 37 GDPA
  - il trattamento è effettuato da **un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali**;
  - le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono **il monitoraggio regolare e sistematico degli interessati su larga scala**; oppure
  - le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento, su larga scala**, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.
- Chi?
- Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
- Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
- Cosa fa? Art. 39 GDPR
  - È coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
  - la raccolta di informazioni per individuare i trattamenti svolti;
  - 'analisi e la verifica dei trattamenti in termini di loro conformità, e
  - l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

SENTENZA TAR FRIULI VENEZIA GIULIA – REQUISITI GIURIDICI DEL DPO

- Sent. 135 del 2018 Reg. Gen. del 13/09/2018
- La certificazione di Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC/27001 può essere requisito necessario per svolgere l'incarico di DPO?
- Il ruolo del Dpo (data protection officer) e' eminentemente giuridico
- Sul punto va rilevato che la certificazione non costituisce un titolo abilitante ai fini dell'assunzione e dello svolgimento delle funzioni di responsabile della sicurezza dei dati, nell'alveo della disciplina introdotta dal GDPR, dovendosi considerare che:
  - da un lato, la norma ISO 27001 trova prevalente applicazione nell'ambito dell'attività di impresa;
  - la minuziosa conoscenza e l'applicazione della disciplina di settore restano, indipendentemente dal possesso o meno della certificazione in parola, il nucleo essenziale ed irriducibile della figura professionale ricercata mediante la procedura selettiva intrapresa dall'Azienda, il cui profilo, per le considerazioni anzidette, non può che qualificarsi come eminentemente giuridico.







Nadina Foggetti

Università degli Studi di Bari A. Moro. *nadinafoggetti@gmail.com*