I requisiti per la nomina del *Data Protection Officer* e la certificazione Lead Auditor ISO 27001

Alida Cilona

Tar Friuli-Venezia-Giulia, 13 settembre 2018, n. 287

Il Tar per il Friuli-Venezia Giulia, con sentenza n. 287/2018 si è soffermato sui requisiti di competenza del Responsabile della Protezione dei Dati personali, nuova figura introdotta dal Regolamento Europeo n. 2016/679, analizzando, in particolare, l'idoneità della certificazione Lead Auditor/Auditor ISO 27001 a costituire requisito essenziale per la nomina del medesimo.

Sommario

1. Premessa. – 2. Il caso. – 3. I requisiti del DPO ai sensi del GDPR. – 4. GDPR e certificazioni in materia di protezione dei dati personali. – 5. La certificazione ISO/IEC 27001:2013. – 6. Conclusioni.

Keywords

GDPR, DPO, Protezione dati personali, Certificazioni GDRP, ISO 27001

1. Premessa

Con sentenza n. 287/2018 depositata il 13 settembre 2018, il Tribunale Amministrativo Regionale per il Friuli-Venezia Giulia si è pronunciato, tra i primi, sul tema dei requisiti per la nomina del responsabile per la protezione dei dati personali previsto ai sensi degli artt. 37 e seguenti del Regolamento (UE) 2016/679 ("GDPR").

2. Il caso

Il tribunale amministrativo è stato chiamato a pronunciarsi sulla legittimità dell'avviso pubblico di un'Azienda Sanitaria finalizzato all'affidamento di un incarico di collaborazione professionale per il ruolo di Responsabile della Protezione dei Dati personali (o *Data Protection Officer* - DPO) con il quale l'ente disponeva la selezione per titoli, ed eventuale colloquio, di un esperto sulla normativa e sulla prassi in materia di protezione dei dati personali per l'impostazione e lo svolgimento nella fase di prima applicazione dei compiti di responsabile della protezione dei dati.

Con riferimento ai requisiti per la partecipazione, l'avviso richiedeva il possesso, in capo a ciascun candidato, del diploma di laurea in Informatica o Ingegneria Informatica, ovvero in Giurisprudenza o equipollenti, nonché la certificazione di Auditor/Lead

Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC 27001.

L'avviso, unitamente al decreto con il quale ne era stata disposta la pubblicazione, veniva impugnato con ricorso da uno dei due soggetti candidatisi alla selezione, laureato in giurisprudenza ma privo della certificazione Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC 27001, senza attendere la determinazione dell'Amministrazione relativamente alla propria domanda.

Chiedendo l'annullamento degli atti amministrativi per «violazione degli artt. 37 e 39 del Reg. UE n. 679/2016; eccesso di potere per violazione di atti di regolazione; eccesso di potere per violazione di atto presupposto; eccesso di potere per manifesta illogicità ed irrazionalità dei requisiti di partecipazione alla selezione; eccesso di potere per sviamento», il ricorrente contestava la pertinenza, rispetto al ruolo da ricoprire, della «certificazione Auditor/Lead Auditor ISO/IEC/27001» richiesta dall'avviso, ritenendo che tale titolo, oltre a risultare privo di attinenza riguardo alle mansioni specificamente richieste dal GDPR e agli stessi compiti enunciati nell'avviso (e, in particolar modo, a quei compiti complementari ivi testualmente indicati), avrebbe determinato un'indebita sperequazione ai danni dei soggetti titolari della laurea in Giurisprudenza, i quali, ove ne fossero stati sprovvisti, non avrebbero potuto partecipare alla selezione per difetto dei requisiti richiesti.

Il ricorrente censurava, peraltro, anche la riconducibilità delle competenze necessarie per l'incarico di DPO alla laurea in informatica o in ingegneria informatica, indicate in avviso quali titoli alternativi alla laurea in giurisprudenza.

L'Amministrazione si costituiva resistendo nel merito e, nelle more del procedimento, si esprimeva con verbale sulla selezione dei candidati ritenendo non ammissibile la domanda presentata del ricorrente, in quanto privo della certificazione ISO/IEC 27001, e valutando positivamente il curriculum dell'unico altro candidato. L'Azienda sanitaria provvedeva, con decreto del Direttore Generale, alla designazione del responsabile della protezione dei dati decidendo, tuttavia, di assegnare provvisoriamente l'incarico, stante la pendenza del contenzioso, ad un proprio dipendente di ruolo.

Con motivi aggiunti, il ricorrente censurava anche il verbale di selezione ed il decreto di designazione del DPO, ribadendo la contestazione circa l'attinenza della certificazione ISO/IEC/27001 rispetto al profilo oggetto dell'incarico, sicché il possesso di tale titolo non avrebbe potuto assurgere a requisito di ammissione.

Rigettate preliminarmente le eccezioni in rito formulate dall'Azienda resistente (inammissibilità dell'impugnativa per difetto di giurisdizione e per originaria carenza del ricorso e dei motivi aggiunti), il Collegio ha infine sancito, nel merito, la fondatezza dell'impugnazione in relazione alla contestata individuazione della certificazione di Auditor/Lead Auditor ISO/IEC 27001 quale requisito di ammissione alla procedura selettiva.

Il Tar ha, invero, rilevato che «la predetta certificazione non costituisce, come eccepito dal ricorrente, 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" e che "la minuziosa conoscenza e l'applicazione della disciplina di settore restano, indipendentemente dal possesso o meno della certificazione in parola, il nu-

cleo 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».
La sentenza ha, pertanto, statuito che la certificazione di Auditor/Lead Auditor ISO/IEC 27001, di per sé, non può costituire requisito di selezione del responsabile per la protezione dei dati personali, in quanto essa non coglie appieno la specifica funzione di garanzia insita nell'incarico conferito, il cui precipuo oggetto non è costituito dalla predisposizione dei meccanismi volti ad incrementare i livelli di efficienza e di sicurezza nella gestione delle informazioni, ma attiene alla tutela del diritto fondamentale dell'individuo alla protezione dei dati personali indipendentemente dalle modalità della loro propagazione e dalle forme di utilizzo.

3. I requisiti del DPO ai sensi del GDPR

Il regolamento (UE) n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, noto come GDPR (*General Data Protection Regulation*), entrato in vigore il 24 maggio 2016 e pienamente applicabile nei Paesi membri UE dal 25 maggio 2018, ha introdotto la nuova figura del Responsabile della Protezione dei Dati personali o DPO (*Data Protection Officer*), come disciplinata dagli artt. 37 e seguenti.
Già, prima d'ora, presente in altri Stati membri dell'Unione (Germania, Austria, Francia), il *Data Protection Officer* previsto dal GDPR ha il ruolo di assistere il titolare ed il responsabile del trattamento nell'applicazione della normativa in tema di protezione dei dati personali, assolvendo ad un ruolo di garanzia della conformità al Regolamento europeo, e più in generale alla normativa in tema di *data protection*, delle attività di trattamento dei dati.
Il Responsabile della Protezione dei Dati personali deve essere obbligatoriamente designato dal titolare o dal responsabile del trattamento dei dati nei casi previsti dall'art. 37 del GDPR:

- 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;
- 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.

In ogni altro caso, il DPO può essere designato in via facoltativa.
La figura di cui agli artt. 37 e seguenti del GDPR può essere un dipendente del titolare o del responsabile del trattamento, oppure un soggetto esterno, anche persona giuridica, sulla base di un contratto di servizi.
Il DPO, comunque individuato, deve poter adempiere alle sue funzioni in piena in-

dipendenza e in assenza di conflitti di interesse (considerando 97 del GDPR) e deve poter disporre di risorse ed autonomia sufficienti a svolgere in modo efficace i compiti di cui è responsabile (art. 38 GDPR).

L'art. 39 del GDPR individua i compiti essenziali del Responsabile della Protezione dei Dati Personali attraverso un elenco non tassativo che può essere ampliato dal titolare o dal responsabile in funzione della specifiche necessità di assistenza e tutela dei dati personali trattati.

Il DPO ha la funzione di:

- informazione, consulenza ed assistenza nei confronti del titolare e del responsabile del trattamento circa gli obblighi derivanti dal Regolamento e dalla normativa nazionale ed europea in materia di protezione dei dati personali;
- sorveglianza dell'osservanza di questi obblighi da parte del titolare e del responsabile del trattamento;
- fornire, dove richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati personali;
- cooperare con l'autorità di controllo e fungere da punto di contatto con essa.

Ai sensi dell'art. 37, par. 5, del GDPR, 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'art. 39.

Allo stato attuale, tale riferimento normativo è l'unico a fornire indicazioni circa i requisiti che debbano essere valutati dal titolare e dal responsabile del trattamento ai fini della designazione del DPO.

Non sono, invero, previsti, nel contesto nazionale od europeo, albi o altri organismi professionali che disciplinino i titoli od i percorsi formativi necessari per svolgere la funzione di Responsabile della Protezione dei Dati Personali, in ambito privato così come in ambito pubblico.

Attraverso le linee guida sui responsabili della protezione dei dati adottate il 13 dicembre 2016 ed emendate il 5 aprile 2017 (WP 243 rev.01), il Gruppo di Lavoro articolo 29 (*Article 29 Working Party*) ha fornito ulteriori indicazioni a titolari e responsabili del trattamento al fine di una corretta valutazione delle competenze del DPO designando. In particolare, secondo quanto indicato dall'*Article 29 Working Party* e rispetto ai requisiti indicati dall'art. 37 del GDPR:

- il livello di conoscenza specialistico richiesto deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento;
- le qualità professionali devono attenere alla conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione di dati, conoscenza che deve essere approfondita con riferimento al GDPR. È utile la conoscenza e familiarità del DPO con lo specifico settore di attività e struttura organizzativa del titolare, nonché con i sistemi informativi e le specifiche esigenze di sicurezza e protezione dei dati del caso specifico. Nel caso di un'autorità o organismo pubblico, il DPO dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili;
- la capacità di assolvere ai suoi compiti deve essere valutata sia con riferimento alle

qualità personali del DPO, anche in termini deontologici, sia con riferimento alla posizione del responsabile all'interno dell'azienda o dell'organismo.

È, pertanto, onere del titolare o del responsabile della protezione dei dati valutare compiutamente le conoscenze specialistiche del soggetto da designarsi, nonché la sua idoneità ad assolvere le funzioni previste dall'art. 39 del GDPR.

Va da sé che la designazione di un Responsabile della Protezione dei Dati personali che difetti delle qualità professionali, delle conoscenze e della capacità richieste per l'assolvimento dei compiti correlati alla funzione, non consentirebbe di ritenere assolto l'obbligo previsto dal Regolamento Europeo e comporterebbe l'applicazione delle sanzioni previste in caso di verifica da parte dell'Autorità di controllo.

4. GDPR e certificazioni in materia di protezione dei dati personali

L'art. 42 del Regolamento Europeo 2016/679 prevede che gli Stati membri, le autorità di controllo, il comitato e la Commissione Regolamento UE 2016/679 dispongano ed incoraggino l'istituzione di meccanismi per la certificazione della protezione dei dati personali, nonché di sigilli e marchi, allo scopo di dimostrare la conformità dei trattamenti effettuati dai titolari e dai responsabili del trattamento.

Ai sensi del GDPR, l'adesione ai codici di condotta o a un meccanismo di certificazione possono, invero, essere utilizzati come elemento per dimostrare il rispetto degli obblighi del titolare o del responsabile del trattamento.

Ai sensi dell'art. 42 GDPR, la certificazione può essere rilasciata direttamente dal Garante ovvero da un organismo nazionale di accreditamento, che in Italia è rappresentato da Accredia (Ente Unico Nazionale designato dal Governo in base al Regolamento CE n. 765/2008), come disposto dall'art. 2-*septiesdecies* del d. lgs. n. 196/2003, come modificato dal d. lgs. n. 101/2018.

Allo stato attuale, non sono ancora stati pubblicati i criteri di accreditamento, i quali devono essere individuati dalle autorità di controllo o dal Comitato Europeo per la Protezione dei dati, né i requisiti per l´accreditamento degli organismi di certificazione.

Con un comunicato congiunto del 18 luglio 2017, il Garante per la protezione dei dati personali e Accredia hanno precisato che «[…] al momento, le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell´adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell´accreditamento degli organismi di certificazione e i criteri specifici di certificazione».

Con riferimento, per quanto qui ci occupa, alla qualifica di *Data Protection Officer*, non risultano, quindi, essere stati ancora individuati dei meccanismi che consentano di certificare la conformità al Regolamento Europeo dei percorsi formativi, oggi variamente ed ampiamente diffusi sul mercato, finalizzati alla preparazione delle competenze spe-

cifiche che il Responsabile della Protezione dei Dati personali deve possedere ai sensi dell'art. 37 GDPR.

5. La certificazione ISO/IEC 27001:2013

La ISO/IEC 27001:2013 (comunemente, anche solo ISO 27001) è uno standard internazionale che definisce i requisiti e le regole per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System).
Lo standard, che trova applicazione per qualsiasi organizzazione che gestisca dati ed informazioni - quindi anche, e soprattutto, organizzazioni diverse da quelle aziendali - si compone di un insieme di requisiti che si prepongono l'obiettivo di garantire Riservatezza, Disponibilità e Integrità delle informazioni (c.d. RID), al fine di garantirne la sicurezza, intesa come la difesa delle caratteristiche delle stesse, nonché dei documenti che le contengono.
Tale obiettivo è perseguito applicando gli opportuni controlli ("*controls*"), annoverati nell'Annex A della norma, al perimetro fisico e logico dell'organizzazione che deve garantire la sicurezza delle informazioni da essa gestite.
L'applicazione di questi controlli (dichiarata nel documento di applicabilità *SOA - Statement Of Applicability*), la valutazione dei rischi (intesa come analisi delle probabilità di accadimento di eventi che possano compromettere una delle caratteristiche di sicurezza delle informazioni e del potenziale impatto degli eventi stessi), la definizione ed implementazione delle contromisure finalizzate alla loro riduzione e la valutazione del rischio residuo costituiscono i principali elementi caratterizzanti questa norma internazionale.
Tra i controlli di conformità sono annoverati anche quelli che fanno riferimento ai requisiti contrattuali e cogenti, come le normative ed i regolamenti, ivi compresa la normativa in materia di protezione dei dati personali (Controllo A.18.1.4 - Privacy e Protezione dei dati personali).
La certificazione di Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni – ISO/IEC 27001:2013 può essere conseguita in esito ad un percorso di formazione, finalizzato all'acquisizione della conoscenza dei contenuti e requisiti dello standard, ed un esame certificati secondo gli standard ISO.
Per via dei suoi contenuti, in larga parte sovrapponibili ai principi del GDPR in tema di sicurezza del trattamento, che richiedono al titolare ed al responsabile di assicurare su base permanente la riservatezza, l'integrità, la disponibilità dei dati e la resilienza dei sistemi e dei servizi di trattamento (art. 32 GDPR), è invalsa l'opinione che lo standard ISO/IEC 27001 possa rappresentare un esempio di *standard* da seguire ai fini della *compliance* al Regolamento Europeo 2016/679.

6. Conclusioni

Per espressa previsione del GDPR (art. 37), la funzione di Responsabile della Protezione dei Dati personali richiede una conoscenza specifica della normativa, nazionale ed europea, in tema di protezione dei dati personali ma anche delle prassi in materia di protezione dei dati personali.
Come sottolineato dalla sentenza in commento, il ruolo di garanzia che il GDPR affida al *Data Protection Officer (DPO)* richiede anzitutto un'approfondita conoscenza della disciplina giuridica in tema di *data protection*, a tutela del diritto fondamentale degli interessati alla protezione dei dati personali.
Sotto tale profilo, appare quindi condivisibile la conclusione cui è pervenuto il Tribunale, secondo cui la conoscenza di *standard* o *best practice* tecniche-organizzative di gestione e sicurezza delle informazioni, seppure approfondita e qualificata, non può essere, di per sé sola, considerata sufficiente a soddisfare appieno i requisiti di competenza del Responsabile della Protezione dei Dati personali.
Tale pronuncia non deve, tuttavia, portare gli interpreti a ritenere che la competenza richiesta al DPO possa prescindere da conoscenze di natura diversa da quella giuridica. Se un'approfondita conoscenza del Regolamento Europeo 2016/679 e dell'insieme di norme nazionali ed europee in materia di protezione dei dati personali costituisce il presupposto imprescindibile per l'espletamento del ruolo di garanzia affidato al Data Protection Officer, la competenza rispetto alle misure tecniche ed organizzative di protezione dei dati costituisce, nondimeno, un requisito essenziale per l'assolvimento dei compiti indicati dall'art. 39 del GDPR.
Ai sensi dell'art. 37 GDPR, il Responsabile della Protezione dei Dati personali deve essere individuato sulla base delle conoscenze specialistiche della normativa, ma anche delle prassi in materia di protezione dei dati personali; ed è proprio il riferimento alla conoscenza delle prassi a suggerire che il DPO debba possedere competenze anche rispetto al funzionamento dei sistemi informativi ed alle misure di sicurezza tecniche ed organizzative di protezione dei dati.
In difetto di competenze di tal natura, il DPO non potrebbe verosimilmente essere in grado di assistere il titolare nel rispetto degli obblighi in materia di protezione dei dati personali, né di sorvegliare compiutamente l'osservanza al GDPR.
Ed è proprio la multidisciplinarietà delle competenze che si richiedono al Responsabile della Protezione dei Dati che porta a ritenere che la designazione di tale figura dovrebbe, opportunamente, riguardare non un singolo soggetto ma, più realisticamente, un team di professionisti (se del caso, attraverso un fornitore esterno di servizi) in grado di offrire competenze nei molteplici ambiti di conoscenza richiesti dal Regolamento Europeo 2016/679, soprattutto laddove l'organizzazione del titolare o del responsabile del trattamento abbiano carattere di complessità.
In tale prospettiva, la certificazione di Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle informazioni – ISO/IEC 27001:2013 può certamente essere valutata positivamente ai fini della designazione del *Data Protection Officer*, ferme restando le necessarie competenze giuridiche che non possono difettare nel profilo di funzione.
È auspicabile che, nell'attività di determinazione dei criteri e meccanismi di certificazio-

ne previsti dagli artt. 42 e 43 GDPR, le autorità di controllo pongano la loro attenzione anche sulla formazione e sulle qualifiche caratterizzanti la figura del *Data Protection Officer*, anche al fine di indirizzare correttamente i titolari ed i responsabili del trattamento nell'assolvimento dell'obbligo derivante dagli artt. 37 e seguenti del GDPR.