

Il ruolo del Data Protection Officer nelle pubbliche amministrazioni

di Marianna Mazzearella

La crescente condivisione di dati personali con le pubbliche amministrazioni richiede un controllo sempre più incisivo sull'effettiva protezione di questi da parte del Responsabile della protezione dei dati, ruolo istituito con il GDPR del 2016.

pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale - 4 giugno 2020

Tra le principali novità conseguenti alla **digitalizzazione della pubblica amministrazione** è rilevante menzionare l'istituzione del ruolo di **Responsabile della protezione dei dati (RPD)**, noto anche come **Data Protection Officer (DPO)**. Tale figura è stata introdotta dall'articolo 37 del **Regolamento generale sulla protezione dei dati (GDPR)**, 2016/279, ed è disciplinata nei due articoli seguenti, in vista dell'applicazione del principio di *accountability*.

Come previsto dalla normativa richiamata, il titolare e il responsabile del trattamento dei dati personali devono designare obbligatoriamente un Responsabile della protezione dei dati quando il **trattamento è effettuato da un'autorità pubblica o da un organismo pubblico**, ad esclusione delle autorità giurisdizionali nell'esercizio delle loro funzioni. Conformemente alle disposizioni nazionali sono, pertanto, tenute a rispettare tale obbligo di designazione le amministrazioni dello Stato, anche con ordinamento autonomo, Regioni ed enti locali, enti pubblici non economici nazionali, regionali e locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti e altri. Si ritiene preferibile che anche soggetti privati che esercitino funzioni pubbliche incarichino un *DPO*.

L'articolo 37 del *GDPR* prevede l'obbligo di designazione di un *DPO* anche quando le attività principali del titolare o del responsabile del trattamento consistono in trattamenti che per natura, ambito di applicazione o finalità richiedono che gli interessati siano monitorati regolarmente e sistematicamente su larga scala; e anche quando gli stessi soggetti svolgono principalmente attività di trattamento, su larga scala, di particolari dati sensibili dei singoli.

Al fine di eseguire al meglio le funzioni cui è adibito, il soggetto in questione deve possedere i requisiti di **terzietà e indipendenza** e, infatti, non deve ricevere istruzioni capaci di orientare le sue decisioni. Qualora, quindi, il ruolo di Responsabile della protezione dei dati sia attribuito ad un soggetto interno alla stessa amministrazione, è preferibile che sia un dirigente o un alto funzionario, in grado di garantire la propria autonomia e la massima collaborazione con il responsabile o il titolare del trattamento. Non mancano, tuttavia, situazioni di **possibili conflitti di interesse** in capo al *DPO*, soprattutto qualora esso ricopra lo stesso ruolo per più autorità o organismi pubblici, o

sia un soggetto esterno all'amministrazione stessa. Per lo stesso ordine di motivi non può essere incaricato per ciascun titolare o responsabile del trattamento dei dati più di un *DPO*, che potrà essere unicamente affiancato da alcuni "referenti".

Il *DPO* esercita **attività di supervisione e di consulenza** nei confronti del titolare e del responsabile del trattamento dei dati personali; controlla l'osservanza del *GDPR* e delle disposizioni comunitarie e nazionali in materia di protezione dei dati, e anche l'attribuzione di funzioni e responsabilità al personale di collaborazione. Egli, inoltre, fornisce su richiesta un parere sulla valutazione di impatto sulla protezione dei dati e coopera con l'Autorità Garante. In considerazione, però, della complessità delle amministrazioni, dell'elevato numero di destinatari coinvolti nelle azioni di queste e dell'eterogeneità degli interessi da contemperare, nella prassi il *DPO* è chiamato a verificare che i procedimenti amministrativi siano conformi alle disposizioni riguardanti la protezione dei dati, fungendo da controllore dei procedimenti.

Per ricoprire tale posizione è, dunque, necessario che il soggetto designato posseda adeguate **competenze tecnico-informatiche, ma anche e soprattutto giuridiche** (in tal senso si è pronunciato il [TAR Friuli Venezia Giulia con sentenza 13 settembre 2018, n. 287](#)). In ogni caso il possesso di specifiche certificazioni professionali, non costituisce uno strumento abilitativo allo svolgimento del ruolo di *DPO*: sono, infatti, il titolare o il responsabile del trattamento a valutare i requisiti posseduti.

Se il *DPO* selezionato è interno all'amministrazione per cui deve operare, viene elaborato un atto di designazione *ad hoc*; in caso contrario, viene stipulato un apposito contratto di appalto, contenente anche l'attribuzione dell'incarico. In tali atti devono essere contenute le motivazioni della scelta di quel particolare soggetto e l'indicazione dei criteri impiegati per effettuarla.

Quanto maggiore è la condivisione di informazioni da parte dei privati cittadini con la pubblica amministrazione, tanto più sarà intensa l'attività esercitata dal Responsabile della protezione dei dati.