Consiglio Nazionale delle Ricerche

Il data Protection Officer nella Pubblica Amministrazione

V. Amenta

IIT B4-01/2017

Nota Interna

Marzo 2017

Istituto di Informatica e Telematica

Il *Data Protection Officer* nella Pubblica Amministrazione

Amenta Valentina
Istituto di Informatica e telematica
Consiglio Nazionale delle Ricerche

Indice: 1. L'introduzione della figura del *Data Protection Officer* nel Regolamento UE n. 679/2016. - 2. Alla ricerca delle origini della figura del *Data Protection Officer*. – 3. Questioni problematiche già emerse. – 4. Il DPO e il sistema di certificazione. – 5. Notazione conclusiva.

Premessa

Tra le novità del Regolamento del Parlamento europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (n.679/2016) è generalmente segnalato l'obbligo, per le aziende di grandi dimensioni e per tutte le pubbliche amministrazioni degli Stati Membri, di nominare un Data Protection Officer.

Non si tratta però di una vera novità, dato che la designazione del DPO è già prevista come obbligatoria da oltre dieci anni nelle istituzioni dell'Unione Europea (regolamento 2001/45/CE); da alcuni anni anche in diversi Stati Membri la nomina del DPO è obbligatoria, mentre in altri è facoltativa.

In vista dell'entrata in vigore del regolamento (prevista per il 2018), l'intervento si propone di analizzare la pregressa esperienza, muovendo dall'esame della legge tedesca ("Legge per lo sviluppo dell'elaborazione e della protezione dei dati personali" del dicembre 1990, come modificata nel 2001 e nel 2010), al fine di tracciare i connotati di questa nuova figura obbligatoria per gli enti pubblici.

Saranno oggetto di specifica considerazione la nomina del DPO "interno" e del DPO "esterno" all'ente pubblico e all'azienda privata e la giurisprudenza lavoristica tedesca (specificamente la decisione del Tribunale del lavoro superiore regionale dello Stato di Sassonia del 14 febbraio 2014) in relazione a controversie che hanno avuto ad oggetto DPO dipendenti aziendali.

Si proveranno poi a tracciare i confini delle responsabilità posta in capo al DPO e i compiti e le relative responsabilità degli altri soggetti del trattamento (titolare, responsabile, incaricato).

1. L'introduzione della figura del *Data Protection Officer* nel Regolamento UE n. 679/2016.

Per fornire risposte all'evoluzione tecnologica e alla transnazionalità delle questioni giuridiche poste dal mercato digitale europeo in materia di trattamento dei dati personali, il legislatore comunitario, lo scorso maggio, ha emanato il Regolamento n. 679/2016, che abroga la direttiva 95/46/CE.

Tra le novità presenti all'interno del Regolamento vi è l'introduzione del *Data Protection Officer*[1], che in realtà non è una innovazione novità assoluta, posto che in alcune legislazioni europee tale figura era già presente.

Il DPO è un supervisore indipendente che sarà designato da soggetti apicali sia delle pubbliche amministrazioni sia in ambito privato. Sarà obbligatorio nelle pubbliche amministrazione e negli enti pubblici: in ambito privato, sarà obbligatorio nelle imprese con 250 dipendenti o più e in particolare quando, tenendo conto dell'ambito applicativo, della natura e delle finalità, il trattamento riguarderà un monitoraggio regolare e sistematico di dati personali su larga scala, oppure se l'attività principale del titolare implicherà un trattamento su larga scala di dati sensibili oppure giudiziari.

A seconda del contesto in cui dovrà operare, il DPO si troverà ad affrontare questioni giuridiche e tecniche-informatiche più o meno complesse, dovendo essere in grado di gestire questioni transnazionali sia all'interno dell'Unione Europea (*rectius* Spazio Economico Europeo, che come noto include oltre agli Stati Membri dell'EU anche il Liechtenstein, l'Islanda e la Norvegia) sia fuori dalla stessa.

Per ricoprire questo ruolo, il Titolare del Trattamento o il Responsabile del Trattamento potranno avvalersi di un proprio dipendente (che sarà dunque un soggetto interno all'impresa), oppure stipulare un contratto di servizi, affidando pertanto tale ruolo ad un soggetto esterno. Il ruolo del DPO dovrà essere ricoperto dallo stesso soggetto per due anni, rinnovabili. Saranno il Titolare o il Responsabile del Trattamento a dover mettere a disposizione le risorse finanziarie e umane necessarie per l'adempimento dei compiti del DPO.

In definitiva, il DPO è un professionista con ruolo aziendale (sia esterno che interno) che deve possedere adeguate competenze giuridiche, informatiche, di analisi dei rischi e dei processi. Le sue principali responsabilità, secondo il disposto dell'art. 39 del Regolamento in oggetto, saranno:

a) informare e fornire consulenza al Titolare o al Responsabile del trattamento nonché ai

[1] Cfr. Sezione 4 del Reg. UE 2016/679, rubricata "*Responsabile della protezione dei dati*".

dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dallo stesso Regolamento e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del Titolare o del Responsabile del trattamento in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del Regolamento;

d) cooperare con l'Autorità garante per la protezione dei dati personali;

e) fungere da punto di contatto con la stessa Autorità garante per questioni connesse al trattamento.

2. Alla ricerca delle origini della figura del *Data Protection Officer*.

Se volessimo ricercare le radici storiche di questa figura dovremo spostarci oltreoceano, quando, nell'agosto1999. la società AllAdvantage (sita in California), specializzata in servizi pubblicitari attraverso Internet, investe il proprio avvocato della carica di *Data Protection Officer*. Nel giro di pochi anni e quindi sul finire del 2001, 500 aziende americane avevano attribuito il ruolo di *Data Protection Officer* ad alcuni dei propri dirigenti. In virtù di questa spinta propulsiva si costituì un'organizzazione di categoria per i "professionisti della *privacy*", la *International Association Of Privacy Professionals*. Questa organizzazione è presente con una sua figura istituzionale anche in Europa, in aggiunta a dei presidi in diversi Paesi del Mondo.

In Europa, si comincia a parlare del DPO con la Direttiva 95/46/CE, che non prevede l'obbligatorietà di tale figura professionale, sebbene alcuni Stati dell'Unione l'avessero già ufficializzata.

In attuazione dell'art. 18 della Direttiva 95/46/CE, la Germania e la Slovacchia, che ha praticamente ricalcato la legislazione tedesca, hanno implementato la figura del DPO come obbligatoria (in Austria si stava avviando la procedura per renderlo obbligatorio prima dell'emanazione del nuovo Regolamento). In altri Paesi come Francia, Olanda, Svezia, è invece previsto il DPO ma come figura facoltativa.

L'introduzione della figura del DPO nella legislazione tedesca ha radici lontane. E' con la "legge per lo sviluppo dell'elaborazione e della protezione dei dati personali" del

dicembre 1990 che si comincia a delineare tale figura. L'art. 36 del *Bundesdatenschutzgesetz*[2], che sancisce la nomina del *Data Protection Officer*[3], sembra anticipare il nuovo regolamento comunitario, che pare ad esso ispirarsi.

Tra i requisiti che deve possedere un soggetto per diventare DPO, il secondo comma dell'art. 36 del BDSG richiede la necessaria conoscenza specialistica in materia di protezione dei dati, oltre che caratteristiche di affidabilità rispetto al tipo di incarico che lo stesso deve ricoprire.

Nell'organigramma aziendale la sua figura è collocata direttamente dietro al proprietario, al consiglio di amministrazione, all'amministratore delegato o ad un gestore legalmente nominato.

Il DPO è tenuto al segreto sull'identità dell'interessato al trattamento dei dati e anche su ogni informazione che potrebbe rivelarne l'identità, salvo che il soggetto stesso esoneri il DPO da tale obbligo di segretezza.

Naturalmente, l'azienda che ha nominato il DPO è tenuta a fornire ad esso ogni attrezzatura e risorsa necessaria per lo svolgimento delle sue funzioni. In particolare l'azienda o l'ente deve fornire al DPO le informazioni affinché questo possa svolgere al meglio il proprio controllo e possa garantire il rispetto delle leggi. Deve nello specifico fornire un elenco contenente: i sistemi di elaborazione utilizzati per il trattamento, la denominazione ed i tipi di file contenenti i dati, la tipologia dei dati memorizzati, i motivi collegati all'attività lavorativa per cui si è resa necessaria la conoscenza di tali dati, i destinatari di tali dati ed, infine, l'indicazione di chi è autorizzato ad accedere ai dati.

Sia che il DPO venga scelto tra soggetti interni all'azienda sia che esso risulti esterno, sarà un soggetto indipendente all'interno dell'organizzazione: ciò è quanto si evince dal fatto che gli unici soggetti ai quali sarà tenuto a riferire saranno solo coloro che rappresentano il "più alto livello di gestione". Questa previsione è presente in tutti gli ordinamenti che hanno in qualche modo previsto questa figura, se ne distacca però la legislazione slovacca che attribuisce al Responsabile del trattamento il compito di formare professionalmente il DPO. Stando alla lettera della legge, dunque, in Slovacchia chiunque può essere nominato DPO, anche senza una formazione specifica che può avvenire in un secondo momento. Quindi non è riscontrabile il grado di indipendenza del ruolo svolto dal DPO. La Slovacchia dovrà provvedere ad un aggiornamento di tale normativa anche perché nel nuovo regolamento comunitario è

[2] Legge 1990 BGBI.I.S.2954, modificata nel 2001 e nel 2010.
[3] Identificato come "*Beauftragter fur den Datenschutz*".

espressamente previsto che a tutela dell'autonomia e indipendenza del DPO nello svolgimento del proprio incarico, allo stesso non deve essere impartita alcuna istruzione per quanto riguarda l'esecuzione dei compiti di propria competenza.

Il quadro normativo delinea, dunque, il *Data Protection Officer* come una figura manageriale (executive manager), di consulenza e controllo, assimilabile, per taluni aspetti e per i requisiti di autonomia e indipendenza, alle funzioni che esercita – sebbene in un diverso contesto - un Organismo di Vigilanza istituito ai sensi della L. n. 231/1991. Il DPO, infatti, funge sia da *auditor* sia da referente per la protezione dei dati e per la gestione degli adempimenti previsti per il corretto trattamento dei dati personali nel contesto dell'ente pubblico o dell'organizzazione privata in cui opera.

Il nuovo regolamento si distacca dalla legislazione tedesca in merito all'obbligatorietà di tale figura.

Secondo la legislazione tedesca, ripresa anche da quella slovacca, i soggetti pubblici devono obbligatoriamente nominare un DPO se impiegano più di nove persone per elaborare automaticamente i dati o più di venti persone per elaborare manualmente i dati[4].

Inoltre, indipendentemente dal numero di persone occupate ai fini dell'elaborazione automatica dei dati, tutti gli enti non pubblici[5] devono implementare tale figura se trattano dati per il loro trasferimento commerciale (ad esempio, gli scambi di indirizzi), per ricerche di mercato, ovvero se trattano dati sensibili (ad esempio, i dati sull'origine razziale o etnica, sulle opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute e la sessualità) e se compiono attività di profilazione della personalità dell'interessato, a meno che non abbiano ricevuto il suo consenso.

Il nuovo regolamento comunitario non prevede distinzione fra elaborazione automatica e non automatica dei dati personali, ma fa ricorso al concetto di "larga scala",

---

[4] Cfr. Sezione 4 *Vierter Abschnitt Sondervorschriften*, art. 42*, Datenschutzbeauftragter der Deutschen Welle: "Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit tritt. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden […]Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Welle alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluss eines Organes der Deutschen Welle. Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit".*

[5] Intendendosi per tali le persone giuridiche, le società per azioni o società a responsabilità limitata, le società di persone, le associazioni senza personalità giuridica (ad esempio i sindacati o partiti politici), le persone fisiche libere professioniste (ad esempio medici, architetti, avvocati).

prevedendo la presenza del DPO quando il trattamento riguarderà un monitoraggio regolare e sistematico di dati personali su larga scala. E' evidente che assume specifica rilevanza la definizione del concetto di "larga scala"[6], in assenza di precisazioni normative sul numero di trattamenti di dati personali che ne possano integrare il significato. Sarebbe forse parso preferibile quantificare un numero di base, ad esempio, ipotizzare una cifra minima di 500, 1000 o 2000 trattamenti annuali, potenzialmente variabile da uno Stato Membro all'altro.

Al momento, fra gli Stati Membri dell'Unione Europea, solamente alcuni (fra cui Germania, Francia, Belgio, Paesi Bassi, Norvegia, Svezia e Regno Unito) prevedono una raccomandazione circa la nomina di un DPO, ciò ad indicare la mancanza di un'armonizzazione a livello europeo che il Regolamento si prefissa di colmare. Vi è comunque il rischio che tale gap legislativo non venga colmato in presenza di concetti non chiariti come quello in esame.

Relativamente alle soluzioni a tale lacuna normativa vi è senza dubbio la possibilità di una definizione del concetto di 'larga scala' da parte delle istituzioni europee oppure un accordo comune da parte degli Stati Membri circa il numero minimo di trattamenti da considerare su 'larga scala' sia nei casi di elaborazione automatica che non. Affinché si arrivi ad un'armonizzazione generale del Regolamento, è necessario che tale lacuna venga affrontata al più presto da esperti in materia e istituzioni nazionali ed europee in modo che ogni Stato Membro si possa adeguare alla normativa, senza alcuna necessità di libera interpretazione, prima della vigenza del Regolamento.

3. Questioni problematiche già emerse.

Alcune problematiche legate a questa figura sono già emerse, nella prassi tedesca, a partire dalla sua collocazione nell'organigramma aziendale, che si è già detto potrà essere propria di un dipendente ovvero di un soggetto reclutato dall'esterno.

Nella legislazione tedesca risulta anzitutto palese come non sia richiesta nessuna particolare certificazione per svolgere l'attività. Una volta nominato, il mandato del DPO dura 12 mesi, rinnovabili e la risoluzione dell'incarico può avvenire solo per "importanti ragioni". Il licenziamento per "importante motivo" richiede una grave

[6] Cfr. Art. 37, Regolamento UE 2016/679, rubricato "Designazione del responsabile della protezione dei dati": Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: […] c) 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 […].

violazione dei doveri contrattuali, come ad esempio la commissione di un reato penale; di conseguenza, molto raramente i tribunali emetteranno una sentenza che accerti l'avvenuta risoluzione del rapporto di lavoro. Proprio per questo, e in assenza di una certificazione che attesti l'effettiva conoscenza del lavoratore, risulta molto problematico per le aziende tedesche nominare il candidato ideale. Sicuramente, come si evince dal parere del *Dusseldorfer Kreis*, ossia l'autorità che raccoglie i Garanti tedeschi, si esclude che il ruolo di DPO possa essere assunto dal responsabile delle risorse umane o dei settori di sicurezza e tecnologia aziendale.

In merito, di notevole rilevanza è la sentenza del Tribunale del lavoro superiore regionale dello Stato di Sassonia del 14 febbraio 2014[7]. Nel caso di specie, una società impegnata nella fornitura di servizi IT aveva assunto l'attore come "*System engineer* e consulente", sulla base di un contratto di lavoro che prevedeva tra i compiti specifici anche lo svolgimento dell'attività di DPO. Secondo l'accordo, però, la necessaria nomina ufficiale come *Data Protection Officer* avrebbe dovuto essere effettuata in una fase successiva. La società ha contestato al dipendente la bassa prestazione entro il

[7] *Court ruling of the Higher Regional Labor Court of the state of Saxony*, February 14, 2014 (3 Sa 485/13):
The employer—an entity engaged in the provision of IT services—hired the claimant as a "system engineer and consultant" on the basis of an employment agreement, which determined, inter alia, that the employee was to carry out "the tasks of a data protection officer." According to the agreement, however, the necessary official appointment as DSB would be carried out "at a later stage."[…]. But things turned out differently: The Company dismissed the employee for low performance within the six month probation period and, in particular, before the official appointment took place. Until termination date the employee undisputedly performed the tasks typically assigned to a DSB.
This gave rise to a claim for unlawful dismissal filed by the employee who argued that such dismissal was invalid due to his factual activity as DSB. According to the employee, he could not be treated any different solely because of the lack of an official appointment; after all, he performed contractual services just like an appointed DSB. The refusal of legal protection would unlawfully compromise the required independence of a DSB which is explicitly and strongly protected by the BDSG, and would lead to a circumvention of the rigid protection against dismissal granted to the DSB by German statutory law. If his claim would be denied, it would be in the employer's sole discretion to postpone the beginning of such protection and to weaken the DSB's position and the fulfilment of his duties. As a result, according to the employee, although his probation had not ended by the time notice was rendered, the performance of the tasks of a DSB would make the dismissal unlawful […]. The Higher Regional Labor Court of Saxony, however, dismissed the employee's claim and denied him the requested legal protection against dismissals of a DSB. According to the court, the performance of the tasks of a DSB is not an equivalent to the appointment of an employee as DSB; the latter would require the execution of a written document signed by both parties pursuant to Sec. 4 of the BDSG. […]The court did not show any concern that employer and employee can validly agree to carry out the appointment as DSB at a later stage of employment. If the parties decide to take this approach, the statutory protection against dismissal will not be triggered immediately, but only upon official appointment as DSB. The court has chosen a very formal, but clear standpoint that allows employers in particular, to agree with an employee that his appointment as DSB shall be conditional upon the survival of the six-month-probation period. Due to the fundamental significance of the legal problems dealt with in the court ruling, the court, however, explicitly admitted an appeal to the Federal Labor Court (BAG). It will be now up to the BAG to further develop their case-law in the field of data protection law which continues to have a growing effect on German employment law.

periodo di prova di sei mesi e, in particolare, prima della nomina ufficiale come DPO (anche se il lavoratore fino alla data di licenziamento aveva indiscutibilmente eseguito i compiti tipicamente assegnati a tale figura).

Il dipendente sosteneva che il licenziamento fosse illegittimo proprio in forza della sua attività di DPO, il cui svolgimento era evidente dai contratti commerciali che egli aveva stipulato e aveva in essere, nonostante la mancanza di formalizzazione da parte della società.

Il Tribunale del Lavoro d'appello della Sassonia, tuttavia, ha respinto la domanda del dipendente. Secondo il giudice, l'esecuzione dei compiti di un DPO non è un equivalente alla nomina di un dipendente come DPO (quest'ultimo richiede infatti la redazione di un documento scritto firmato da entrambe le parti ai sensi della Sezione 4 della BDSG). Il Tribunale ha adottato, per la soluzione del caso, un punto di vista molto formale e non sostanziale, aprendo la strada alla possibilità dei titolari del trattamento di pattuire un accordo con un dipendente e subordinando la nomina come DPO al superamento del periodo di prova.

Per determinare la responsabilità dei DPO è necessario, quindi, distinguere tra soggetti interni ed esterni. In caso di una violazione da parte di funzionario, si applicheranno - seppure con alcune problematicità - le disposizioni del diritto del lavoro. In questa situazione, le aziende potranno licenziare i DPO solo se gli stessi hanno commesso illeciti intenzionalmente o con negligenze gravi.

Nel caso in cui il titolare scelga una figura esterna all'azienda, lo stesso mantiene l'eventuale responsabilità per violazione della normativa sulla protezione dei dati, non potendo liberarsi da questa situazione per effetto della nomina di un DPO che la commissione di un danno rivela non essere stato sufficientemente istruito.

4. Il DPO e il sistema di certificazione.

Questo problema può essere superato con l'introduzione delle certificazioni. Nelle legislazioni dove il DPO è facoltativo, come quella francese e olandese, possono essere chiamati a svolgere la funzione di DPO solo i soggetti autorizzati da apposite certificazioni, che ne comprovano la professionalità.

Le certificazioni sono rilasciate da enti terzi indipendenti e imparziali accreditati ai sensi della norma internazionale UNI CEI EN ISO/IEC 17024. In Francia un organismo certificatore è TÜV SÜD *France Sas*. Infatti, grazie agli accordi internazionali di mutuo riconoscimento che l'*Agence d'accréditation pour l'enseignement supérieur et le*

Conseil d'accréditation e dal 2008 il Cofrac, hanno stipulato con gli altri enti di accreditamento europei (EA- *European Cooperation for Accreditation*), queste certificazioni godono di un riconoscimento internazionale che ne assicura la piena validità in tutti i principali mercati del mondo. Oltreoceano, questo sistema di misurazione è in effetti utilizzato già da diversi anni, ad esempio IAPP ha sviluppato negli USA un proprio sistema di certificazione per figure quali l'*Information Privacy Manager* (CMP) e l'*Information Privacy Professional* (CIPP), mentre in Canada i professionisti della *Data Protection* si possono accreditare come *Certified Privacy Officer* presso l'*Order of Privacy Officers*.

È chiaro come l'introduzione di figure "certificate" serva non solo a spostare da un soggetto (titolare/responsabile del trattamento) ad un altro (il DPO, appunto) tutta una serie di responsabilità in ambito di protezione dei dati, ma anche e soprattutto consenta di formare soggetti specializzati ed esperti, costantemente aggiornati sui rischi, i problemi e le misure di sicurezza necessarie a garantire un livello di tutela dei dati personali adeguato. Il tutto in linea con l'importanza, la diffusione e la complessità che l'ambito della protezione dei dati personali (soprattutto in campo digitale e tramite web) sta sempre più acquisendo.

Nell'ordinamento francese, rispetto agli altri Paesi, si sta consolidando la prassi di una voluta divisione dei ruoli tra Responsabile del trattamento e DPO, sul filo della distinzione tra attività ordinaria e straordinaria.

L'attività ordinaria rientra nella figura del Responsabile dei dati, così come anche noi in Italia siamo abituati a concepirlo[8]. Essa consiste nella continua e costante tenuta sotto controllo ed aggiornamento del vecchio DPS, nella gestione e valutazione delle attività di formazione, nell'aggiornamento dei regolamenti interni e della documentazione. Annualmente tale figura dovrà predisporre una relazione, nella quale sono descritte le attività svolte e dove si motivano le cause per cui non sono state rispettati, se del caso, alcuni adempimenti. La pianificazione e l'effettuazione dell'attività di *auditing* completano le attività ordinarie che sono poste a carico del DPO.

L'attività straordinaria riguarda, invece, i progetti e gli obiettivi di miglioramento. In questo caso le novità possono essere originate dalla normativa di settore, dalle esigenze dei clienti, dalla direzione o dalle attività che nascono a seguito dello sviluppo di nuovi

[8] Naturalmente rimangono vive le differenze insite nel recepimento della direttiva comunitaria 95/46/CE: la legge italiana prevede un regime particolare per i c.d. dati sensibili (consenso scritto dell'interessato e autorizzazione preventiva del garante), mentre in Francia, la situazione è diversa, in quanto per il trattamento di questi dati si richiede esclusivamente il consenso scritto dell'interessato e nessuna forma di controllo preventivo da parte del CNIL.

prodotti o nuovi servizi che abbiano impatto sugli aspetti connessi alla *Data Protection* e i compiti di indirizzo e di monitoraggio spettano al DPO[9].

Le imprese dovranno quindi, se vorranno raggiungere standard di sicurezza adeguati, nominare tali figure anche laddove ciò non sia obbligatorio per legge, possibilmente affidando tale compito a soggetti terzi ed esterni: il DPO, infatti, riferisce direttamente ai vertici aziendali e non al titolare/responsabile del trattamento (sebbene anche questi ultimi possano essere, nel contesto aziendale, suoi superiori), e nonostante le garanzie di autonomia e indipendenza sancite dalla legge, bisogna chiedersi effettivamente quanti dipendenti potrebbero essere pronti a denunciare comportamenti o valutazioni errate del titolare e del responsabile del trattamento al *top manager*.

5. Notazione conclusiva.

Sarebbe quindi auspicabile una maggiore e più precisa configurazione dei soggetti coinvolti nel trattamento dei dati personali nella Pubblicazione amministrazione.

Il triangolo costruito sulle figure di Titolare, Responsabile ed Incaricato del trattamento dovrà diventare un quadrato che ha per vertici:

I. Il Titolare del Trattamento, ora chiamato *Data Controller* o Responsabile del trattamento, dotato di un potere decisionale in ordine alle tecniche da adottare e alle misure organizzative, al fine di garantire la conformità al Regolamento delle operazioni di trattamento dei dati.
II. Il Responsabile esterno del Trattamento / Amministratore di Sistema, ora chiamato *Joint Controller* o Co-responsabile del trattamento.
III. Il responsabile ed incaricato del trattamento, ora chiamato *Data Processor* e Incaricato del Trattamento o più semplicemente *Data Handler*, sostituisce l'attuale figura del "responsabile del trattamento" conosciuta dalla direttiva abrogata e potrà procedere al trattamento dei dati solo su istruzione del responsabile.
IV. Infine, il responsabile della sicurezza dei dati, ora chiamato *Data Protection Officer*.

[9] Il quale deve costantemente aggiornare lo stato del progetto rispetto ai vari parametri di controllo; al termine dovrà redigere un consuntivo. Dinanzi a progetti complessi il DPO deve essere in grado di individuare le priorità che non sono fornite necessariamente dalle scadenze, ma dall'urgenza delle stesse, intervenendo in modo tempestivo e risolutivo.