Responsabile privacy, profilo a prova di dubbi

La nuova figura debutta il 25 maggio: ecco i chiarimenti del Garante per le imprese e i professionisti

Antonello Cherchi

Un elenco, semplificativo ma comunque chiarificatore, di quanti devono rispettare l'obbligo e di chi, invece, non è tenuto; la precisazione che, se individuato all'esterno dell'impresa, può trattarsi anche di una persona giuridica; l'indicazione che un gruppo aziendale può anche designare un unico soggetto, purché facilmente raggiungibile da ogni stabilimento.

Sono alcune delle risposte che il Garante della privacy ha fornito per aiutare i privati (imprenditori, liberi professionisti, fondazioni, società, banche, ma anche partiti, sindacati e Caf) a mettere meglio a fuoco il profilo del Dpo (*data protection officer* o responsabile della protezione dei dati), la nuova figura prevista dal regolamento europeo 2016/679 che diventerà operativo il prossimo 25 maggio.

Progettare la privacy

Si tratta di un ruolo importante, perché funzionale al nuovo concetto di privacy disegnato dalle regole Ue, disposizioni che tra poco meno di due mesi varranno per tutti i Paesi dell'Unione senza le declinazioni nazionali conosciute fino a oggi. Un impianto che fa perno sul concetto di *accountability*, ovvero l'attenta valutazione di tutti i rischi privacy connessi a una particolare situazione e la predisposizione di adeguate misure di protezione. Interventi da tenere sempre aperti per poterli aggiornare sulla base degli eventuali cambiamenti nella struttura organizzativa o per adeguarli alle novità tecnologiche. Progettualità e flessibilità che i recenti fatti di Facebook dimostrano quanto mai necessaria per non doversi trovare a fronteggiare disastrose perdite di dati personali.

Ecco perché il Dpo deve possedere una conoscenza adeguata dei processi di gestione delle informazioni e deve agire in piena autonomia nel garantire il rispetto da parte della struttura in cui opera del regolamento europeo e del resto della normativa privacy. Altro compito è quello di fungere da cerniera tra il proprio datore di lavoro e il Garante della privacy. Non sono necessari - come il Garante aveva già avuto modo di chiarire - particolari titoli di studio o abilitazioni. Non c'è, in altri termini, un "bollino" che certifichi il profilo del Dpo.

Di certo, sarà una figura particolarmente richiesta da qui ai prossimi mesi. Si stima ne serviranno 40mila, tra quelli da impiegare nella pubblica amministrazione e gli altri necessari nel settore privato.

Cantiere aperto

Se per il Dpo "pubblico" il Garante aveva già fornito alcune indicazioni, sempre attraverso le Faq, per imprese e professionisti, invece, i chiarimenti erano attesi. Dai diversi incontri che l'Autorità guidata da Antonello Soro ha fatto con le associazioni di categoria, infatti, sono giunte richieste di chiarimenti. Quelle pubblicate in pagina - e disponibili da oggi anche sul sito dell'Autorità: www.garanteprivacy.it - sono le prime risposte alle domande più frequenti arrivate da Confindustria piuttosto che da Confcommercio o Confartigianato, Abi, Assaeroporti, Assogestioni, Fca, Enel, Unicredit, Banca Intesa, Rai. Per citare alcune associazioni e imprese con le quali il Garante ha avuto contatti in questi ultimi mesi con l'obiettivo di rendere meno traumatico il passaggio dal vecchio al nuovo sistema privacy.

Si tratta di un primo passo. Il percorso di supporto e collaborazione, infatti, prosegue tanto nei confronti della Pa che dei privati. Altre indicazioni arriveranno nei prossimi mesi, soprattutto per rispondere agli assai probabili problemi applicativi che sorgeranno dopo il 25 maggio.

Intanto, il 24 maggio, il giorno precedente il d-day della privacy, il Garante ha organizzato al Palazzo dei congressi di Bologna un incontro con tutti i Dpo, pubblici e privati, per gli ultimi suggerimenti prima del "primo giorno di scuola".

LE TAPPE. IL PRIMO TEST È CAPIRE SE LA NOMINA VA FATTA

Chi omette la designazione subisce sanzioni pesanti

di **Riccardo** e **Rosario Imperiali**

Dopo le Faq generali del Gruppo di lavoro dell'articolo 29 e quelle del Garante privacy per i Dpo degli enti pubblici, arrivano le Faq per i Dpo dei privati. Una prima linea di demarcazione rispetto all'ambito pubblicistico del ruolo riguarda il profilo dell'obbligatorietà della designazione: obbligatoria è la designazione del Dpo per tutti gli enti pubblici, cioè senza alcun discrimine; mentre obbligatoria lo è per i privati, solo in presenza di determinate circostanze. Il regolamento europeo permette, però, allo Stato membro di prevedere ulteriori casi di obbligatorietà.

Conseguenza pratica derivante da questa diversità di disciplina è la necessità, per il contesto privato, di operare una preliminare valutazione finalizzata a stabilire la sussistenza delle condizioni di legge che fanno scattare tale obbligatorietà. Valutazione delicata, non sempre agevole, foriera di rilevanti conseguenze, in quanto l'omessa designazione del Dpo obbligatorio è sanzionabile amministrativamente con il pagamento di una somma il cui massimo ammontare è pari a 10 milioni di euro ovvero, se superiore, al 2% del giro di affari globale annuo.

La valutazione operata dovrà essere comprovata documentalmente e, nel caso in cui si pervenga a conclusioni di non obbligatorietà, ne andranno evidenziate le argomentazioni, al fine di consentire al Garante di accertare agevolmente il rispetto della prescrizione. Questa documentazione andrà ad arricchire il composito sistema documentale *data protection* che ciascuna azienda titolare del trattamento, e per taluni versi anche se "responsabile", è tenuta a realizzare e mantenere aggiornato, al fine di comprovare la propria *accountability*.

Contrariamente al caso precedente, prive di conseguenze giuridiche saranno le ipotesi opposte di valutazioni che dovessero erroneamente concludere per l'obbligatorietà della designazione, in realtà non dovuta nel caso di specie. La designazione del Dpo è un elemento rafforzativo per la tenuta del sistema data protection aziendale, per cui la designazione volontaria è da accogliere comunque con favore; tant'è che nei casi di dubbia obbligatorietà, le Autorità consigliano di procedere comunque alla designazione.

Di interesse, al riguardo, sono gli esempi forniti nelle Faq, sia in senso confermativo dell'obbligatorietà sia per quelli per i quali appare improbabile tale obbligo. È bene ricordare, comunque, che gli esempi forniti non si sostituiscono alla citata valutazione preliminare, in quanto l'obbligo di designazione sussiste solo in presenza dei presupposti di legge.

La designazione è operazione di innesco per una molteplicità di prescrizioni ulteriori che vanno puntualmente rispettate: a partire dall'evitare confusioni terminologiche con altre figure organizzative affini ma non rispondenti ai requisiti che la legge indica per il Dpo. In proposito, infatti, considerata la funzione di vigilanza non operativa, tipica del ruolo, è plausibile riscontrare la presenza all'interno dell'organizzazione aziendale di un parallelo ruolo operativo privacy; in tal caso, la denominazione attribuita a questa funzione non dovrà risultare ambigua rispetto al diverso ruolo legale del Dpo per evitare il disorientamento degli interessati.

L'avvenuta designazione (sia essa obbligatoria o volontaria) sarà comunicata al Garante utilizzando l'apposito modulo indicato nelle Faq, mentre i dati di contatto vanno pubblicati sul sito web aziendale. Se la scelta cadrà su un interno, oltre alla redazione dell'atto di designazione, si dovrà avere cura di evitare conflitti di interesse con eventuali compiti ulteriori già assegnati alla stessa persona. Se, invece, la scelta riguarderà un esterno, la contrattualizzazione del rapporto di servizio dovrà fornire specifiche indicazioni su compiti, risorse e quant'altro utile per lo svolgimento del mandato nel contesto di riferimento; con l'avvertenza che, anche in caso di contratto con una società, l'individuazione riguardi comunque una persona fisica.

1

Chi è il responsabile della protezione dei dati personali (Rpd) e quali sono i suoi compiti?

Il responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese *"data protection officer"* – Dpo) è una figura prevista dall'articolo 37 del regolamento (Ue) 2016/679. Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del regolamento medesimo. Coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante; si veda la Faq 6) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (articoli 38 e 39 del regolamento).

2

Quali requisiti deve possedere il responsabile della protezione dei dati personali?

Il responsabile della protezione dei dati personali, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.
Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (considerando 97 del regolamento Ue 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici.
Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.

3

Chi sono i soggetti privati obbligati alla sua designazione?

Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'articolo 37, paragrafo 1, lettere b) e c), del regolamento (Ue) 2016/679. Si tratta di soggetti le cui principali attività (in primis, le attività cosiddette di *core business*) consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala" si vedano le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile del trattamento dei dati personali (articolo 37, paragrafo 4).
Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; Caf e patronati; società operanti nel settore delle *utilities* (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

4

Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?

Nei casi diversi da quelli previsti dall'articolo 37, paragrafo 1, lettere b) e c), del regolamento (Ue) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: si veda anche il considerando 97 del regolamento, in relazione alla definizione di attività "accessoria").
In ogni caso, resta comunque raccomandata, anche alla luce del principio di *accountability* che permea il regolamento, la designazione di tale figura (si vedano, in proposito, le menzionate linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

5

È possibile nominare un unico responsabile della protezione dei dati personali nell'ambito di un gruppo imprenditoriale?

Il regolamento (Ue) 2016/679 prevede che un gruppo imprenditoriale (si veda la definizione di cui all'articolo 4, n. 19) possa designare un unico responsabile della protezione dei dati personali, purché tale responsabile sia facilmente raggiungibile da ciascuno stabilimento (sul concetto di "raggiungibilità", si veda il punto 2.3 delle linee guida in precedenza menzionate). Inoltre, dovrà essere in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.

6

Il responsabile della protezione dei dati personali deve essere un soggetto interno o può essere anche un soggetto esterno? Quali sono le modalità per la sua designazione?

Il ruolo di responsabile della protezione dei dati personali può essere ricoperto da un dipendente del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il regolamento (Ue) 2016/679 assegna a tale figura. Il responsabile della protezione dei dati scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.
Nell'esecuzione dei propri compiti, il responsabile della protezione dei dati personali (interno o esterno) dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il titolare o il responsabile del trattamento che abbia designato un responsabile per la protezione dei dati personali resta comunque pienamente responsabile dell'osservanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla (articolo 5, paragrafo 2, del regolamento; si vedano anche i punti 3.2 e 3.3. delle linee guida sopra richiamate).
I dati di contatto del responsabile designato dovranno essere infine pubblicati dal titolare o responsabile del trattamento. Non è necessario - anche se potrebbe rappresentare una buona prassi - pubblicare anche il nominativo del responsabile della protezione dei dati: spetta al titolare o al responsabile e allo stesso responsabile della protezione dei dati, valutare se, in base alle specifiche circostanze, possa trattarsi di un'informazione utile o necessaria. Il nominativo del responsabile della protezione dei dati e i relativi dati di contatto vanno invece comunicati all'Autorità di controllo. A tal fine, allo stato, è possibile utilizzare il modello di cui al seguente link: http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/7322292

7

Il ruolo di responsabile della protezione dei dati personali è compatibile con altri incarichi?

Si, a condizione che non sia in conflitto di interessi. In tale prospettiva, appare preferibile evitare di assegnare il ruolo di responsabile della protezione dei dati personali a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile It, ecc.). Da valutare, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale).

8

Il responsabile della protezione dei dati personali è una persona fisica o può essere anche un soggetto diverso?

Il regolamento (Ue) 2016/679 prevede espressamente che il responsabile della protezione dei dati personali possa essere un "dipendente" del titolare o del responsabile del trattamento (articolo 37, paragrafo 6, del regolamento); ovviamente, nelle realtà organizzative di medie e grandi dimensioni, il responsabile della protezione dei dati personali, da individuarsi comunque in una persona fisica, potrà essere supportato anche da un apposito ufficio dotato delle competenze necessarie ai fini dell'assolvimento dei propri compiti.
Qualora il responsabile della protezione dei dati personali sia individuato in un soggetto esterno, quest'ultimo potrà essere anche una persona giuridica (so veda il punto 2.4 delle suddette linee guida).
Si raccomanda, in ogni caso, di procedere a una chiara ripartizione di competenze, individuando una sola persona fisica atta a fungere da punto di contatto con gli interessati e l'Autorità di controllo.

DOMANDE E RISPOSTE A CURA DEL
Garante per la protezione dei dati personali