Autorizzati al trattamento dei dati personali

written by goal | 7 Gennaio 2019

di Stefano Bacchiocchi*

Una delle figure chiave previste dalla nuova normativa privacy dettata dal GDPR (General Data Protection Regulation) e dal decreto legislativo 10 agosto 2018, n. 101 *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"* è il cosiddetto "autorizzato al trattamento". Spesso, a un professionista che si occupa di privacy, viene chiesto come inquadrare correttamente, nell'ambito dell'organizzazione aziendale o dello studio professionale, dipendenti e collaboratori interni. La risposta probabilmente più corretta è quella di procedere alle nomine di questi soggetti in qualità di autorizzati al trattamento.

Il GDPR indica che non sono considerati soggetti terzi all'organizzazione (oltre a titolare e responsabili ed eventualmente il DPO) anche quelle persone che trattano dati personali sotto l'autorità diretta del titolare o del responsabile. Così come il codice della privacy, anche il GDPR consente la nomina di incaricati al trattamento, chiamati "autorizzati o delegati". Si può dare una definizione molto pratica: gli autorizzati al trattamento sono tutti quei soggetti interni alla organizzazione che nello svolgimento dei loro compiti e delle loro mansioni entrano in contatto con dati personali. Subito dopo aver dato questa breve definizione sorgono i primi dubbi applicativi: ciò è tipico di quando si passa da una visione della privacy come mero adempimento ad

una visione della normativa aziendalistica e prettamente organizzativa; ci si accorge che non c'è nulla di semplice (niente da invidiare ad esempio alle normative antiriciclaggio), ragion per cui le risposte, come per le altre figure e casistiche, sono e devono essere articolate. Per fare delle scelte oculate possiamo dare alcuni spunti con esempi molto pratici al fine di avere uno schema applicativo quanto più possibile definito. Dobbiamo distinguere i dipendenti e collaboratori che non trattano dati personali (di persone fisiche) da quelli che invece trattano questa tipologia di dati. Nel primo caso è evidente come non servirà nessuna nomina o contratto particolare; tuttavia, pur apparendo di semplice soluzione ed inquadramento, la realtà merita un'analisi più approfondita. Se, per esempio, un dipendente lavora in officina ad un tornio ed utilizza schede di lavoro che riportano nomi, cognomi, numeri di telefono ecc. ma per la mansione che svolge non dovrebbe avere questa tipologia di dati: in tal caso c'è un problema non banale di organizzazione, in quanto la scheda della lavorazione non dovrebbe indicare quei dati che devono quindi essere eliminati a monte. In tal caso, tecniche e buone prassi (come minimizzare i dati o usare la pseudonimizzazione) permetterebbero di evitare questo problema. In pratica la scheda lavoro e più in generale i dati trattati devono essere nascosti, codificati o cancellati dalla vista del lavoratore non autorizzato.

Per ovviare al suddetto problema – a volte – si autorizzano "a tappeto" tutti i lavoratori; tuttavia questa soluzione, a parere dello scrivente, non è corretta e può portare a sanzioni o quantomeno ad un processo di trattamento non lineare ed efficiente. Non basta infatti autorizzare questi lavoratori al trattamento dei dati, poiché vige un principio generale della normativa che chiede di "minimizzare" i dati trattati e creare divisioni organizzative di responsabilità; è imperativo quindi autorizzare al trattamento dei dati solo quei lavoratori che necessitano veramente di tali dati per la

mansione svolta. Negli studi professionali, la quasi totalità dei collaboratori e dipendenti appartiene al secondo caso, cioè svolge mansioni che richiedono il trattamento di dati personali di persone fisiche (carte d'identità, numeri di telefono personali, indirizzi, condizioni economiche e sociali, dichiarazioni reddituali ecc.); in questo caso è opportuno nominarli quali autorizzati al trattamento dei dati personali. In verità, la soluzione non è immediata ed automatica neppure in questo caso. Si può giungere a questo tipo di conclusione seguendo un ragionamento logico-giuridico che parte dalla traduzione italiana del GDPR 2016/679, (in vigore del 25 maggio 2018); questa figura infatti non è citata espressamente dalla norma. E' invece citata dall'art.4, n.10 del Regolamento nel seguente disposto: "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile". Anche il Garante italiano, nella guida all'applicazione del Regolamento, considera questo tipo di figura; si trova scritto: <<Pur non prevedendo espressamente la figura dell'incaricato del trattamento (ex art. 30 del d.lgs. n. 196/2003), il regolamento UE non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento)>>.

Quindi nulla vieta che si possa responsabilizzare questi soggetti attraverso un incarico ben definito.

E' consigliabile questa modalità operativa anche in ottica di "best practice" volta a dimostrare ulteriormente l'adeguamento al GDPR. Non solo: quale altro mezzo abbiamo per dimostrare *ex post* che i dipendenti e collaboratori hanno ricevuto istruzioni in tema privacy se non facendo firmare un qualche tipo di documento che lo attesti?

In tema di istruzioni quindi è fondamentale fornire agli autorizzati le istruzioni operative (art. 29 GDPR), compresi gli obblighi inerenti le misure di sicurezza, e che sia

fornita loro la necessaria formazione. In caso contrario, infatti, anche in presenza di formali designazioni, queste sarebbero del tutto prive di valore. La “nomina” degli autorizzati può avvenire anche con unico atto comprensivo di tutti lavoratori; tenendo presente però che la conoscenza dell’incarico e delle istruzioni fornite è fondamentale per l’adeguamento alla normativa, e l’autorizzato dovrà ovviamente attenersi strettamente alle istruzioni ricevute che quindi vanno portate a piena conoscenza dei designati; ecco dunque di nuovo il tema della formazione: non si potrà mai essere aderenti alla normativa senza aver organizzato una formazione adeguata.

Bisogna porre anche attenzione al fatto che la normativa non prevede requisiti quantitativi per essere considerati autorizzati, per cui anche la semplice presa visione di un dato personale (es. chi vede una bolla di consegna) è un trattamento. Non è nemmeno rilevante che il lavoratore sia inserito stabilmente nell’organico dello studio o dell’azienda, ad esempio gli stagisti o gli studenti in alternanza scuola lavoro, se trattano dati personali di persone fisiche, dovrebbero essere inquadrati come autorizzati al trattamento.

È inoltre fondamentale la formazione dei collaboratori e dipendenti poiché non è possibile autorizzare al trattamento soggetti che non hanno idea della normativa o di come siano strutturati i processi interni di acquisizione e trattamento dei dati; questo è tanto più vero quando i collaboratori siano nuovi dell’organico o precari. Da qui il tema di chi o come debba essere fatta la formazione in tema privacy: allo stato attuale della normativa non è stato definito un organo preposto alla formazione né tantomeno delle certificazioni. Si può però dire con certezza che la legge prevede tra gli incarichi affidati al DPO (Data Protection Officer, figura descritta nei precedenti numeri di questa Rivista) anche quello della formazione sia al Titolare del trattamento sia ai

collaboratori e dipendenti: (art 39 punto 1.b) “sorvegliare l’osservanza del presente regolamento, di altre disposizioni dell’Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l’attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo”.

E’ quindi consigliabile che la formazione venga fatta dal DPO (se nominato) o almeno (in attesa di conferme) da un soggetto che ricopra questa carica in altre aziende o enti.

* *Odcec Brescia*