

La struttura di governance

Autore: Redazione

In: Diritto civile e commerciale

Il **DPO** deve aiutare il titolare del trattamento nella corretta individuazione di un **organigramma privacy** che alla fine si ricollega alla definizione di uno specifico modello organizzativo. Come noto diverse sono le figure soggettive che assumono rilevanza nel mondo della protezione dei dati personali. Innanzitutto l'interessato che è definito dall'**art. 4 del Regolamento** come la persona fisica identificata o identificabile e si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Non vi sono, quindi, sostanziali differenze rispetto a quanto previsto dal Codice in materia di protezione dei dati personali e i diritti dell'interessato sono disciplinati dal Capo III del Regolamento. Il titolare del trattamento (art. 4) è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità, le condizioni e i mezzi del trattamento sono determinati dal diritto dell'Unione o dal diritto di uno Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere designati dal diritto dell'Unione o dal diritto dello Stato membro. Nell'ambito dell'organizzazione dell'ente o dell'azienda il titolare del trattamento rimane una figura fondamentale e tale figura assume una rilevanza tale da coincidere con lo stesso concetto di titolare del trattamento di cui al nostro codice. Egli è tenuto ad adottare politiche e attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme alla normativa.

Molte di queste ultime misure sono nuove rispetto alla precedente normativa. Difatti oltre alla **legittima conservazione della documentazione ed all'attuazione dei necessari requisiti di sicurezza dei dati**, è prevista l'esecuzione della valutazione d'impatto sulla protezione dei dati (concetto del tutto nuovo), il rispetto dei requisiti di autorizzazione preventiva o di consultazione preventiva dell'autorità di controllo e del responsabile della protezione dei dati, la designazione di un responsabile della protezione dei dati e la definizione di informazioni e comunicazioni trasparenti da fornire all'interessato. Il titolare del trattamento deve essere in grado di dimostrare l'efficacia di tali misure e ciò nel rispetto dell'importante principio di accountability (già approfondito nel capitolo precedente) che viene recepito dal Regolamento europeo.

La responsabilità del titolare del trattamento

Per lo stesso motivo il Regolamento intende definire una responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che abbia effettuato direttamente o altri abbia effettuato per suo conto. In particolare, il titolare del trattamento deve garantire ed essere in grado di dimostrare la conformità di ogni trattamento con il Regolamento. Altra importante novità connessa alla figura del titolare del trattamento è il recepimento dei principi della **privacy by design** anch'essi approfonditi nel capitolo precedente. Il responsabile del trattamento (**art. 4**) è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento. tale figura è di tutt'altra rilevanza rispetto al passato in quanto il responsabile assume nell'ambito del Regolamento una connotazione quasi professionale. Difatti, dice la norma (**art. 28**) che "qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato". Quindi non viene scelta una persona fisica o giuridica qualsiasi, ma chi possieda già determinate competenze, per cui appare evidente che anche il responsabile del trattamento debba avere una formazione specifica. Inoltre il Regolamento sancisce che l'esecuzione dei trattamenti su commissione è disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto deve prevedere, in particolare, che il responsabile del trattamento: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28. Di conseguenza lo stesso accordo tra titolare ed responsabile del trattamento deve avere un fondamento giuridico in quanto deve essere oggetto di contratto o altro atto giuridico che preveda tutta una serie di obblighi del responsabile che dipende direttamente dal titolare, può impiegare soltanto personale che si sia impegnato alla riservatezza e principalmente viene considerato anch'esso titolare del trattamento qualora tratti dati personali diversamente da quanto indicato nelle istruzioni dal titolare del trattamento. Ciò si intuisce da quanto disciplinato dall'**art. 26 del Regolamento** che parla anche di contitolari del trattamento quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato. È evidente, quindi, che la figura del responsabile del

trattamento è connessa ad un soggetto che grazie al possesso di determinate competenze collabora concretamente con il titolare per la creazione di quelle condizioni tecniche e organizzative necessarie per l'adempimento dell'obbligo del titolare del trattamento di dare seguito alle richieste per l'**esercizio dei diritti dell'interessato**, assumendo peraltro determinate responsabilità derivanti dalla stipula di un accordo contrattuale.

Il consenso dell'interessato

Proprio per questi motivi lo stesso Regolamento specifica che il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati **se non è istruito in tal senso dal titolare del trattamento**. tra i vari obblighi, inoltre, il Regolamento pone a carico del responsabile, ma anche del titolare del trattamento l'obbligo di conservazione della documentazione di tutti i trattamenti effettuati sotto la propria responsabilità. Conservazione che se riferita a documenti informatici ovviamente implica necessarie competenze inerenti la conservazione sostitutiva. Inoltre l'**art. 28 del GDPR** chiarisce che quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile. In merito va rilevato che recentemente la legge europea n. 167 del 20 novembre 2017 aveva dettato alcune disposizioni modificative o integrative del Codice in materia di protezione dei dati personali. In particolare l'art. 28 della legge aveva introdotto il comma 4-bis all'art. 29 del codice in materia di protezione dei dati personali andando ad aggiungere al responsabile interno del trattamento disciplinato dai primi 4 commi anche la figura del responsabile esterno così come disciplinata dall'**art. 28 del regolamento europeo n. 2016/679 (GDPR)**. Difatti viene prevista la possibilità per il titolare del trattamento, in conformità a quanto previsto dal regolamento comunitario, di avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2. In tal caso i titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento; i predetti atti verranno adottati in conformità a schemi tipo predisposti dal Garante. tale difficile situazione di commistione, in realtà è stata superata con il decreto legislativo di adeguamento al GDPR che ha abrogato in toto il preesistente art. 28 del Codice prevedendo all'art. 2-quaterdecies che il titolare o responsabile del trattamento possano prevedere sotto la propria responsabilità e nell'ambito del proprio assetto

organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. È chiaro il riferimento di questa disposizione sia al responsabile interno che all'incaricato figure che il Regolamento non contempla nello specifico ma che alla fine possono continuare regolarmente ad esistere, Per ragioni di mera opportunità forse adesso sarebbe il caso di definirli autorizzati al trattamento dei dati personali ma con diversi profili di responsabilità.

Il presente contributo è tratto:

<https://www.diritto.it/la-struttura-governance/>