Ruoli, governance e responsabilità per la gestione della privacy

A domanda risponde Prof. Avv. Michele IASELLI

8 maggio 2024 - dalle ore 15.00 alle 16.00

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54
Web: www.dpoinrete.it
www.asmel.eu

Definizione di un organigramma privacy

La definizione di un organigramma privacy è un passo cruciale nell'ambito della gestione della protezione dei dati personali all'interno di un'organizzazione.
Un organigramma privacy non è solamente un diagramma organizzativo, ma rappresenta la struttura attraverso la quale si definiscono i ruoli e le responsabilità legati alla privacy e alla protezione dei dati.

Obiettivi dell'organigramma privacy

- **Chiarezza dei ruoli**: Specificare chiaramente le figure rilevanti con riferimento ai vari livelli organizzativi.
- **Definizione delle responsabilità**: Dettagliare le responsabilità specifiche di ciascun ruolo, inclusi la raccolta, l'elaborazione, la sicurezza e la divulgazione dei dati personali.
- **Facilitare la conformità normativa**: Assicurare che l'organizzazione rispetti la normativa sulla privacy come il GDPR, identificando chiaramente chi deve agire e come per l'adempimento delle prescrizioni normative.

Figure previste

Titolare del trattamento

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 é 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.

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, il rispetto dei requisiti 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 che viene recepito dal GDPR. 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 per cui lo stesso titolare tenuto conto dell'evoluzione tecnica e dei costi di attuazione, deve mettere in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme al Regolamento e assicuri la tutela dei diritti dell'interessato. In particolare, se all'interessato è lasciata facoltà di scelta relativamente al trattamento dei dati personali, il titolare del trattamento garantisce che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite.

Responsabile del trattamento

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.

E’ 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.

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.

Contitolarità del trattamento

L’art. 26 del Regolamento 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.

Referente o delegato del titolare del trattamento

Non va confusa con la figura del responsabile del trattamento quella prevista dall'art. 2-quaterdecies del codice in materia di protezione dei dati personali introdotto dall'art. 2 del d.lgs. n. 101/2018 che reca una serie di disposizioni volte a precisare taluni poteri e obblighi in capo al titolare e al responsabile, tra cui la possibilità di delegare compiti e funzioni a persone fisiche operanti sotto la loro autorità e responsabilità.

Tale disposizione assume una particolare rilevanza proprio perché risolve in parte le diverse problematiche sorte a seguito di quanto stabilito dall'art. 28 del GDPR che concepisce il solo responsabile esterno del trattamento.

Incaricato o autorizzato al trattamento

Nulla dice il Regolamento in merito alla figura dell'incaricato così come la conosciamo nel nostro Codice per la protezione dei dati personali e l'arcano è presto chiarito. Difatti la figura dell'incaricato scompare a seguito della traduzione-interpretazione in lingua italiana proposta dalla nostra Autorità Garante alla Commissione Europea ed accettata da quest'ultima.
Difatti secondo l'ormai superata Direttiva 95/46/CE il "controller" era il nostro "responsabile de trattamento", mentre il "processor" era il nostro "incaricato". A seguito, invece, della proposta del Garante, alla luce dell'attuale Regolamento, per "controller" bisogna intendere "titolare del trattamento", mentre per "processor" bisogna intendere "responsabile del trattamento".

Comunque è pacifico che, a prescindere da aspetti di carattere terminologico, l'incaricato debba necessariamente continuare ad esistere, anche se sarebbe preferibile chiamarlo in modo diverso, ad esempio autorizzato al trattamento.

La figura del Responsabile della Protezione dei dati (RPD | DPO)

Tra le maggiori novità del Regolamento Europeo sulla protezione dei dati personali rientra sicuramente la previsione del Data Protection Officer (DPO) o responsabile della protezione dei dati, figura professionale di indubbio rilievo.

La previsione normativa

In effetti l’art. 37 del Regolamento prevede che quando:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali, oppure
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9 (dati sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10
il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati (c.d. data protection officer).

Qualora, poi, il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

Il DPO è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai propri compiti. Tale figura, di alto livello professionale, può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure adempiere ai suoi compiti in base a un contratto di servizi e quindi può essere un libero professionista.

Il DPO deve essere prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali sia dal titolare del trattamento che dal responsabile del trattamento e gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal Regolamento.

Il DPO deve godere di ampia autonomia e non riceve alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti. Inoltre il Regolamento specifica (art. 38) che il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti, ma riferisce direttamente ai massimi superiori gerarchici del titolare del trattamento o del responsabile del trattamento.

Quali sono i compiti del DPO?
(art. 39 del Regolamento)

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché 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 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;

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

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Linee-guida sui responsabili della protezione dei dati (RPD) del WG 29 adottate il 16 dicembre 2016 ed emendate in data 5 aprile 2017.

Attività DPO

Conoscere tutti gli aspetti organizzativi dell’ente: il DPO deve necessariamente analizzare ed approfondire i compiti e le funzioni fondamentali dell’ente che assiste. Tale attività è fondamentale per consigliare nel modo migliore il titolare o responsabile del trattamento.

Mappare e classificare i trattamenti dati con un occhio particolare ai dati che vengono trasferiti all'estero ed a eventuali accordi di carattere contrattuale (binding corporate rules).
In genere questo tipo di attività viene svolto attraverso la diretta compilazione dei registri delle attività di trattamento che, come già si è avuto modo di vedere, per quanto considerate a livello di Regolamento attività proprie del titolare e del responsabile del trattamento, alla fine vengono curate dallo stesso DPO, più che altro, per ragioni di opportunità.

Individuare un organigramma privacy e prevedere un coordinamento funzionale, ai fini privacy, tra i diversi uffici della realtà organizzativa. Si tratta di un aspetto delicato ma fondamentale che può consentire allo stesso DPO di individuare con immediatezza eventuali problematiche che dovessero insorgere nell'ambito dell'azienda o ente.

Prevedere specifiche policy del trattamento dei dati e fornire attività di consulenza in tale settore con un'attenzione particolare rivolta all'utilizzo delle nuove tecnologie (videosorveglianza, biometria, Rfid, big data, uso della rete per attività di marketing, profilazione, posta elettronica aziendale, sistemi automatici decisionali ed utilizzo dell'IA, tecnologie robotiche, cloud computing, IoT, ecc.).

Analizzare l’impatto delle predette nuove tecnologie in ambito protezione dei dati personali al fine di fornire specifica consulenza al titolare del trattamento per la predisposizione di un DPIA.

Aiutare il titolare del trattamento nel predisporre un’efficace politica di sicurezza informatica.
A tal fine sarà necessario dare utili suggerimenti in merito anche alla definizione di programmi di formazione ed aggiornamento per tutti gli operatori (autorizzati) e naturalmente per i referenti del titolare.

Curare, tramite il titolare del trattamento, i rapporti con gli interessati al fine di fornire risposta adeguata a determinate richieste di chiarimenti in materia o a reclami/ricorsi.

Supportare il titolare del trattamento nella predisposizione di specifici report di data breach e nelle relative comunicazioni agli interessati.

Aiutare il titolare del trattamento nella predisposizione e gestione di specifici audit privacy interni ed esterni.

Mantenersi aggiornati con riferimento alla normativa nazionale ed europea in materia di protezione dei dati personali confrontandosi nel caso anche con altri DPO.

Curare i rapporti con l’Autorità garante su tutte le tematiche che dovessero investire l’azienda o l’ente in materia di privacy.

Monitorare in generale tutte le attività di trattamento dati al fine di assicurare il rispetto della normativa nella specifica realtà organizzativa di riferimento.

Amministratore di sistema

In materia di trattamento e protezione dei dati, l'Amministratore di Sistema rappresenta una figura chiave, considerato l'ambito e la delicatezza della propria operatività, sempre più bersaglio di attacchi informatici e digitali di ogni genere. A livello organizzativo, tale soggetto riveste un ruolo fondamentale nel sistema di *accountability*, in quanto con la sua nomina il Titolare del trattamento assegna ad un determinato soggetto (sia esso interno all'organizzazione sia esso in *outsourcing*) la gestione e la manutenzione della struttura IT aziendale, nonché l'adozione di opportune misure di sicurezza, rilevando in particolare nella fase di *privacy by design*.

Resta tutt'ora valido quanto statuito dal Garante per la Protezione dei Dati Personali, con il Provvedimento del 27 novembre 2008, modificato poi con il Provvedimento del 26 giugno 2009, relativo alle "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema* Garante per la Protezione dei Dati Personali, "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

Il Garante della Privacy in tale contesto ha stabilito che gli Amministratori di Sistema sono "*in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti*", inoltre aggiunge che "*vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi*".

Sempre il Garante, ha ulteriormente precisato che l' "*amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali*".

È opportuno precisare che il Garante ha escluso da tale accezione tutti coloro che svolgono le prestazioni sopra indicate in modo occasionale e solo per scopi di manutenzione tecnica a seguito di specifici malfunzionamenti, nonché gli “operatori di sistema”, in quanto, in questo caso, gli Amministratori di Sistema hanno una rilevanza superiore, possedendo privilegi maggiori e più specifici, rappresentandone sostanzialmente una categoria specifica.

Governance in materia di privacy

La governance della privacy si riferisce al sistema di politiche, procedure, e responsabilità che regolano la raccolta, l'uso, la conservazione e la divulgazione di dati personali all'interno di un'organizzazione. Questo concetto è essenziale per garantire che tutte le attività legate al trattamento dei dati personali siano condotte in modo trasparente, sicuro, e conforme al GDPR.

- **Politiche di privacy**: Creazione di politiche chiare e comprensibili che delineano come i dati personali devono essere trattati e protetti. Queste politiche dovrebbero includere dettagli su quali dati vengono raccolti, perché vengono raccolti, come vengono usati, e come vengono protetti.
- **Procedimenti di gestione dei dati**:
  1. Sicurezza dei dati: Implementazione di misure tecniche e organizzative per proteggere i dati personali da accessi non autorizzati, perdite o distruzione. Questo include la cifratura dei dati, l'uso di firewall, e la realizzazione di backup regolari.
  2. Accesso ai dati e controllo: Definizione di chi può accedere ai dati personali e sotto quali condizioni, garantendo che solo il personale autorizzato possa accedere ai dati necessari per le loro funzioni lavorative.
- **Ruoli e responsabilità**: Predisposizione di un organigramma.
- **Adempimenti:** DPIA, Registro attività di trattamento.
- **Gestione dei consensi**: Assicurare che i consensi siano raccolti in modo informato e esplicito, e che gli interessati possano facilmente ritirare il loro consenso in qualsiasi momento.
- **Audit e monitoraggio**: Effettuare audit interni e/o esterni regolari per valutare l'efficacia delle misure di protezione dei dati e la conformità con le politiche di privacy.
- **Risposta a violazioni dei dati**: Avere un piano chiaro e procedure di risposta per gestire eventuali violazioni dei dati, compreso la notifica agli interessati e alle autorità di regolamentazione, se necessario.