MANAGEMENT

Audit e GDPR

Manuale per le attività di verifica e sorveglianza del titolare e del DPO (Data Protection Officer)

Giancarlo Butti,
Maria Roberta Perugini

FRANCOANGELI

Am - La prima collana di management in Italia

Testi advanced, approfonditi e originali, sulle esperienze più innovative
in tutte le aree della consulenza manageriale,
organizzativa, strategica, di marketing, di comunicazione,
per la pubblica amministrazione, il non profit...

Am - La prima collana di management in Italia

Testi advanced, approfonditi e originali, sulle esperienze più innovative
in tutte le aree della consulenza manageriale,
organizzativa, strategica, di marketing, di comunicazione,
per la pubblica amministrazione, il non profit...

Giancarlo Butti,
Maria Roberta Perugini

Audit e GDPR

Manuale per le attività di verifica e sorveglianza del titolare e del DPO (Data Protection Officer)

FRANCOANGELI

Progetto grafico di copertina di Elena Pellegrini

A Bob (Penna Bianca)

A mia moglie
Alle mie bimbe (Lara, Hope, Chery)
e ai miei bimbi (River, Book, Eros)
Giancarlo

Indice

Introduzione

Dopo oltre un anno dall'entrata in vigore del GDPR (Regolamento (UE) 2016/679)[1] e del relativo adeguamento della normativa italiana sulla protezione dei dati personali, si deve affrontare il tema delle verifiche:

- delle azioni intraprese al fine di garantire la conformità alla normativa;
- del fatto che le policy, le procedure, le misure di sicurezza definite, siano effettivamente implementate e rispettate.

Gli attori coinvolti in tali attività sono:

- il titolare, *cioè la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali...*;
- il responsabile, *cioè la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*;
- il DPO *(Data Protection Officer – Responsabili della protezione dei dati personali), designato ai sensi degli artt. 37-39 del GDPR*.

Le attività di verifica sono svolte di norma da auditor professionisti, siano essi interni o esterni all'azienda, risorse particolamente specializzate e rare.

Nondimeno il compito di sorvegliare il rispetto della normativa è un obbligo dei DPO, che nella maggior parte dei casi si trova ad affrontare questa attività per la prima volta e non dispone, di norma, di adeguati strumenti e competenze per svolgerla.

1. 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Ecco quindi l'idea di questo libro, il cui obiettivo di è quello di consentire:

- sia ad "auditor" professionisti, sia a soggetti che conoscono la normativa privacy, ma che hanno poca dimestichezza con le attività di verifica di:
  - svolgere un assessment in ambito privacy;
  - definire un piano di audit;
  - definire un programma di audit;
  - creare check list;
  - raccogliere evidenze;
  - valutare le risultanze dell'audit;
  - stilare un verbale di audit;
  - …

  al fine di verificare il livello di conformità della organizzazione sottoposta a verifica;
- ai titolari e responsabili, di saper valutare:
  - quali tipi di verifica meglio siano rispondenti alle loro esigenze;
  - le offerte su attività di verifica, distinguendo in particolare fra quelle che si limitano a considerare gli aspetti formali da quelle che effettuano un riscontro oggettivo su come opera l'organizzazione.

Il libro inoltre, anche se limitatamente ai casi trattati, fornisce dettagli sulle implementazioni richieste per garantire la conformità alla normativa.

Gli autori, un auditor professionista con competenze in ambito ICT, organizzativo, legale ed un avvocato con oltre 25 anni di esperienza in ambito privacy, sviluppano i vari temi legati alle verifiche in ambito privacy nelle due parti in cui è organizzato il testo.

Nella prima parte viene affrontato il tema di come impostare un'attività di verifica in generale e più specificatamente in ambito organizzativo e tecnico, mentre nella seconda parte vengono affrontati temi prettamente legali.

Molti degli esempi sono tratti dai miei articoli su Toolnews, e di questo ringrazio Alessandro Giacchino. Un ringraziamento particolare al prof. Fabio Maccaferri, per il suo contributo sul rischio di audit.

Gli eventuali testi delle normative e di altri documenti riportati nel libro hanno solo finalità indicativa e non hanno alcun valore ufficiale.

Gli unici testi ufficiali delle normative sono quelli pubblicati sulla Gazzetta Ufficiale della Repubblica Italiana e Gazzetta Ufficiale dell'Unione Europea che prevalgono in caso di discordanza.

Grazie anche a Leonardo, il Nasci, Deborah e Mario, attenti lettori e suggeritori e soprattutto a Francesca, che ha da subito creduto in quest'opera.

Parte prima

di *Giancarlo Butti*

1 Le verifiche in ambito privacy

Si è volutamente utilizzato il termine verifiche e non audit in quanto non tutte le verifiche sono necessariamente strutturate sotto forma di audit; la normativa privacy, infatti, non prescrive alcuna regola in merito alle modalità con cui effettuare le verifiche.

Spetta quindi al singolo titolare o responsabile del trattamento di dati personali (nel seguito per semplificare si utilizzerà solo il termine titolare anche se quanto esposto riguarda sia i titolari, sia i responsabili, salvo che diversamente specificato) determinare quali siano le modalità con cui vuole effettuare delle verifiche.

Analoga responsabilità investe il DPO, che fra i suoi compiti deve:

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.

Nel complesso le attività di verifica possono riguardare:

- l'autovalutazione della conformità agli adempimenti prevista dalla normativa effettuati dal titolare tramite strutture interne (audit/compliance) o esterne;
- la valutazione della conformità agli adempimenti prevista dalla normativa effettuati dal DPO anche per il tramite di strutture interne (audit/compliance) o esterne;
- la valutazione effettuata da un titolare sugli adempimenti contrattuali del responsabile;
- la valutazione effettuata da un titolare sugli adempimenti messi realmente in atto dal DPO, rispetto a quanto formalizzato nel suo atto di designazione;
- la valutazione effettuata da un titolare sulle caratteristiche di un DPO, rispetto a quanto previsto dalla normativa.

Le attività di verifica non sono codificate in modo puntuale nella normativa e quindi possono essere svolte con una certa libertà di metodo; è tuttavia consigliabile, nel caso si svolgano attività classificabili come audit, utilizzare linee guida e standard codificati da associazioni di settore riconosciute o da organismi di normazione.

Le verifiche possono essere classificate come:

- assessment di carattere generale;
- ricognizioni che portino a formulare suggerimenti in luogo di rilievi[1];
- audit veri e propri;
- verifiche di carattere tecnico;
- verifiche nell'ambito della sicurezza tramite vulnerability assessment e penetration test;

e possono variare in funzione del perimetro sottoposta a verifica:

- processi;
- requisiti normativi;
- …

e della profondità:

- verifiche dei soli aspetti formali (verifica di impianto);
- verifiche della reale operatività messa in atto dall'organizzazione sottoposta a verifica (verifica di funzionamento).

1. Chi effettua le verifiche

L'attività di verifica può essere svolta da personale interno o esterno alla struttura verificata, purché tale personale:

- abbia le necessarie competenze tecnico/giuridiche e conosca i processi ed i trattamenti in essere presso la struttura da verificare;
- non operi in conflitto di interessi, andando a verificare processi o ambiti nei quali è intervenuto lui stesso in fase di implementazione;
- sia adeguatamente supportato nella sua attività di verifica;
- non debba verificare, se interno, una struttura dalla quale dipende gerarchicamente;
- non subisca delle ritorsioni in conseguenza delle sue attività di verifica.

Leggendo queste indicazioni non può mancare un accostamento alle analoghe caratteristiche che deve avere un DPO, ed in effetti la figura del DPO e quella dell'auditor hanno diversi punti in comune.

1. Con il termine rilievo in questo libro si intende il dare evidenza di una differenza fra quanto si è riscontrato in sede di verifica e quanto ci si attendeva.

Nel caso in cui esista un DPO le attività di verifica possono essere svolte direttamente da lui medesimo, in quanto compiere verifiche come abbiamo visto sopra è uno dei suoi compiti (la capacità di svolgere attività di verifica è una delle competenze che il DPO deve possedere).

Nondimeno un titolare potrebbe non avere l'obbligo di designare un DPO, ma disporre di strutture interne dedicate alle attività di verifica.

Tale situazione si presenta comunque molto raramente e riguarda strutture molto grandi e nella maggior parte dei casi specificatamente regolamentate in questo ambito.

Un ottimo esempio di questo caso è l'ambito bancario (dove è anche obbligatoria la presenza di un DPO), che utilizzeremo più volte nel corso del testo.

Non può svolgere attività di verifica un consulente o un'azienda di consulenza che abbia partecipato all'attività di implementazione del modello privacy dell'organizzazione.

Vi sarebbe altrimenti un palese conflitto di interessi.

Nel caso in cui l'attività sia svolta da parte di una società di consulenza, vi è conflitto di interessi anche nel caso in cui chi svolge le attività di verifica sia una persona che non ha partecipato alle attività di consulenza (si troverebbe nella scomoda posizione di dover valutare l'operato dei colleghi).

Un comportamento difforme da qunto appena descritto:

- è eticamente scorretto;
- pone dei rischi per la conformità del titolare, che deve essere in grado di dimostrare il motivo delle sue scelte;
- pone dei rischi operativi per il titolare, in quanto difficilmente chi ha implementato un modello privacy secondo i propri criteri ne evidenzierà i limiti in sede di verifica.

2. Le caratteristiche di chi svolge le verifiche

Vari istituti, tra cui, *in primis*, The Institute of Internal Auditors e ISACA, hanno emesso delle linee guida e degli standard per lo svolgimento delle attività di audit e indicato le caratteristiche che devono avere i soggetti che svolgono tale attività[2].

Ad esempio gli Standard Internazionali dell'Internal Auditing e le Guide Interpretative per la Pratica Professionale, la cui traduzione italiana è curata dall'AIIA (Associazione Italiana Internal Auditor) elenca i seguenti standard di connotazione:

1100 – Indipendenza e Obiettività;

2. Per approfondimenti su questo tema e sugli standard relativi alle attività di audit si rimanda alle pubblicazioni delle citate istituzioni.