Giancarlo Butti, Maria Roberta Perugini, 2019, Franco Angeli

AUDIT E GDPR – MANUALE PER LE ATTIVITÀ DI VERIFICA E SORVEGLIANZA DEL TITOLARE E DEL DPO

Le attività di **verifica ed audit**, oltre a costituire un obbligo per i DPO, sono uno strumento di **accountability per tutti i titolari e responsabili del trattamento.**

Il volume affronta il tema delle verifiche in ambito privacy evidenziando le peculiarità determinate da una normativa particolarmente articolata, vasta, trasversale, in continua evoluzione e nella quale i pochi requisiti di conformità definiti in modo puntuale (ad esempio, il contenuto obbligatorio dell'informativa) coesistono con i molti la cui valutazione è lasciata alla responsabilità del Titolare (ad esempio, le misure di sicurezza).

Il volume descrive dunque il processo di audit nel suo complesso: la stesura di un piano di audit, la definizione di una metodologia di descrizione delle non conformità, la loro valutazione secondo diverse metodologie (quali ad esempio modelli di maturità), la stesura di un audit report e la relativa valutazione complessiva.

Dopo una presentazione delle caratteristiche dell'attività di audit e dei relativi standard e buone pratiche, il **volume propone metodologie per effettuare un assessment iniziale utile a individuare le aree a maggiore rischio di non conformità e a definire il conseguente piano di audit.**

Vengono proposte metodologie di verifica dei requisiti di conformità attraverso check list precostituite, ma anche suggerimenti su come **costruire check list personalizzate** ed altri strumenti utili nei documenti realizzati da Enti, Agenzie e Autorità Garanti, quali esempi di buone pratiche.

Vengono descritti sia **i punti di controllo di carattere generale**, che caratterizzano una normativa che impone ai titolari di essere in grado di dimostrare in ogni momento la propria conformità, sia quelli specifici di ogni macro argomento trattato.

Gli obiettivi del libro sono molteplici:

- 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.
- consentire a Titolari e Responsabili di 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 (verifiche di impianto) da quelle che effettuano un riscontro oggettivo su come opera l'organizzazione (di funzionamento).
- fornire, anche se limitatamente ai casi trattati, dettagli sulle implementazioni richieste per garantire la conformità alla normativa.

Un breve capitolo analizza anche le varie figure coinvolte: chi può svolgere un'attività di verifica, le qualifiche che deve avere, le certificazioni esistenti per dimostrare le proprie competenze. ■