RATIO QUOTIDIANO
Il commento e la critica delle più importanti notizie del momento

DIRITTO PRIVATO, COMMERCIALE E AMMINISTRATIVO

di BARBARA GARBELLI

Audit privacy: perché evitare le domande che orientano la risposta

Durante un audit sulla protezione dei dati, le domande tendenziose compromettono obiettività, indipendenza e valore probatorio delle verifiche. La revisione della ISO 19011 ribadisce l'importanza della neutralità e del metodo nella conduzione delle interviste.

L'audit rappresenta uno degli strumenti centrali per la verifica dell'efficacia dei sistemi di gestione e per la dimostrazione della conformità al GDPR.
La **ISO 19011,** linea guida di riferimento per la conduzione degli audit, è oggi in fase di revisione con pubblicazione prevista nel 2026. Pur senza modifiche sostanziali, il documento rafforza un principio essenziale: **l'audit deve essere condotto in modo imparziale, indipendente e metodologicamente coerente.**
Tra gli aspetti più delicati rientra la **formulazione delle domande durante le interviste,** in particolare quelle che la norma definisce *"leading questions",* in italiano, domande che orientano la risposta.

Perché le domande tendenziose sono un rischio - La sezione A17 della ISO 19011:2018, dedicata alla conduzione delle interviste, distingue tra domande aperte, chiuse, di apprezzamento e orientate. Le domande tendenziose appartengono a quest'ultima categoria: sono quelle che presuppongono un problema, suggeriscono la risposta desiderata e limitano la libertà dell'interlocutore.
Utilizzarle durante un audit significa ridurre l'obiettività del processo e compromettere la qualità delle evidenze raccolte. Esse, infatti, suggeriscono implicitamente la risposta attesa, condizionano l'intervistato e possono generare risposte compiacenti, riducono la capacità dell'audit di far emergere criticità reali e compromettono l'imparzialità e l'indipendenza dell'auditor.
Esempi tipici, in ambito protezione dati, sono domande come: *"Non avete avuto alcun data breach quest'anno, vero?"* oppure *"Presumo che cambiate le password semestralmente, giusto?".* In entrambi i casi, la formulazione condiziona l'intervistato, spingendolo verso una risposta di conferma piuttosto che di analisi.

Effetti sul sistema di gestione e sulla conformità al GDPR - Nel contesto della protezione dei dati personali, la neutralità dell'audit assume valore giuridico. Il principio di accountability (art. 5, par. 2, GDPR) richiede che le organizzazioni dimostrino la conformità in modo oggettivo e documentato.
Un audit basato su domande che orientano la risposta produce invece: report non attendibili, incapaci di rappresentare la realtà operativa; verbali privi di valore probatorio in caso di controllo ispettivo; decisioni errate nelle successive attività di valutazione d'impatto (DPIA) o nella gestione di incidenti di sicurezza.
Di fatto, la formulazione scorretta delle domande può condurre a una falsa percezione di conformità, esponendo l'organizzazione a rischi sanzionatori e reputazionali.

Neutralità e metodo: le chiavi di un audit efficace - L'auditor non deve mai cercare conferme, ma evidenze.
L'intervista deve essere condotta in modo asettico, senza giudizi o complicità con l'auditato.
Il valore dell'audit risiede nella capacità di raccogliere dati oggettivi, basati su risposte spontanee e verificabili. Per questo, le domande più efficaci sono:
- aperte, quando mirano a comprendere processi e comportamenti *("Come gestite gli accessi ai sistemi?");*
- chiuse, quando servono a ottenere conferme specifiche *("Chi autorizza i log di accesso?");*
- di apprezzamento, utili per valutare consapevolezza o percezione *("Come giudica l'efficacia delle attuali misure di sicurezza?").*

Le domande orientate, al contrario, vanno evitate o utilizzate con estrema cautela, solo in contesti mirati e con finalità di verifica puntuale.

Conclusione - La conduzione di un audit sulla protezione dei dati richiede equilibrio tra rigore tecnico e neutralità comunicativa. Domande neutre, formulate con precisione e senza presupposti impliciti, consentono di raccogliere evidenze oggettive, indispensabili per dimostrare la reale conformità dell'organizzazione.