Il principio di privacy-by-design per gestire gli adempimenti previsti dal GDPR

Date : 21 marzo 2018

Negli ultimi mesi si sono moltiplicati gli interventi sul GDPR. L'esperienza con norme dedicate ai sistemi di gestione (in particolare ISO 9001 e ISO/IEC 27001) può aiutare ad attuare alcuni requisiti in modo sì rigoroso, ma anche sostenibile nel tempo.

È infatti evidente che molte guide, suggerendo soluzioni eccessivamente onerose, non tengono conto di come si possa garantire l'adeguatezza degli adempimenti nel tempo. Citando Monica Perego, è necessario un "sistema di gestione per la privacy".

Si presentano nel seguito delle considerazioni su alcuni punti chiave del GDPR.

Termini e definizioni

Chi lavora da tempo con le norme ISO vede che alcune aziende non usano i termini prescritti dalle norme. Molte chiamano "azioni di miglioramento" le "azioni correttive" (o le famigerate, non più richieste, "azioni preventive"), altre parlano di "SAL" al posto di "riesami della progettazione" e così via.

Quindi, se un'azienda è abituata a parlare di "dati sensibili" e non di "categorie particolari di dati personali ai sensi dell'articolo 9 del GDPR", può continuare ad usare la vecchia dicitura, anche più semplice. Stesso discorso per gli "incaricati" (oggi "persone autorizzate al trattamento dei dati personali", che è poi la stessa definizione fornita dal D. Lgs. 196 del 2003). L'importante è sicuramente gestire correttamente i dati sensibili e gli incaricati, considerando le novità del GDPR (e forse è più efficace segnalare i cambiamenti introdotti piuttosto che sproloquiare sulla terminologia).

D'altra parte in molti continuano a dire "informativa", anche se il termine non è presente nel GDPR.

I rapporti con i dipendenti

In questi mesi le aziende stanno aggiornando le informative relative ai trattamenti dei dati dei

propri dipendenti e i regolamenti sulla sicurezza dei dati. Molti si chiedono come distribuire questi documenti e come raccogliere le firme di avvenuta ricezione.

È bene ricordare che non è necessario dimostrare con firma il recapito delle informative e dei regolamenti. Oggi sono disponibili email, bacheche virtuali, sistemi di distribuzione delle buste paga a cui allegare l'informativa e il regolamento aggiornati.

È fondamentale individuare il metodo più efficiente per distribuire questi documenti, soprattutto perché potrebbero essere aggiornati frequentemente.

Fino al 2000, le aziende certificate ISO 9001 mantenevano una lista di distribuzione dei documenti della qualità, con le firme di coloro che ricevevano il manuale (o parte di esso) e le procedure aggiornati. Era un sistema estremamente inefficiente, anche per le piccole aziende, e anche inefficace, visto che non si riusciva quasi mai a raccogliere tutte le firme. Con il tempo, anche i più diffidenti hanno accettato l'uso delle tecnologie e sarebbe opportuno recepire questa esperienza per il GDPR.

Si ricorda che informative e regolamenti vanno distribuiti anche ai collaboratori temporanei, agli stagisti e a tutte le persone che lavorano per l'azienda.

Le nomine a incaricato

In molti si affannano a scrivere nomine a incaricati individuali e, in modo simile alle informative e ai regolamenti, cercare di raccogliere le firme di ciascun destinatario.

Il nostro Codice della privacy già non riteneva necessario questo approccio, considerando come designazione ad incaricato anche "la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima".

In altre parole, familiari a chi conosce sistemi di gestione ISO, è sufficiente pubblicare un organigramma e un mansionario sufficientemente dettagliato. Metodo sicuramente più efficiente ed efficace.

Chi si occupa di ISO/IEC 27001, inoltre, non si ferma qui, ma estende la propria analisi ai processi tecnologici: come viene comunicato l'incarico e le sue modifiche agli amministratori di sistema affinché configurino opportunamente e tempestivamente le autorizzazioni sui sistemi informatici e se è previsto in riesame periodico delle autorizzazioni assegnate (processi previsti dall'Allegato B del D. Lgs. 196, anche per le autorizzazioni per gli archivi fisici, purtroppo spesso ignorati).

Per quanto riguarda la formazione, oggi sono diffusi e validamente usati strumenti di e-learning. Al termine del corso (in aula o a distanza) è possibile richiedere la compilazione di un semplice questionario tecnico, in modo che i partecipanti possano dimostrare di aver recepito i concetti più importanti.

I responsabili (o *processor*)

Oggi sappiamo bene che i “responsabili” sono solo quelli “esterni”. Semplificando, si tratta dei fornitori a cui sono affidati dei trattamenti di dati personali.

I fornitori, però, non sono tutti uguali e pertanto è necessario prevedere contratti diversi per ciascuna categoria, con diverse clausole relative al trattamento dei dati personali.

E’ quindi necessario trovare un metodo per scrivere le clausole in modo da poterle applicare a tutti i fornitori (per esempio, introducendole con frasi come “nel caso di fornitori di servizi informatici”), oppure individuare le tipologie di fornitori a cui le clausole devono essere indirizzate e creare più modelli di riferimento.

Questo approccio è noto nell’ambito della ISO 9001, che richiede di valutare periodicamente i fornitori, considerando le caratteristiche di ciascuno di essi, e dovrebbe essere recepito.

Per quanto riguarda i responsabili “interni”, interpretazioni autorevoli confermano che non sono previsti dal GDPR, né lo erano dalla precedente Direttiva (la sfortunata traduzione di “processor” con “responsabili” ha alimentato la confusione in Italia). In molti si stupiscono e si chiedono come possa essere possibile distribuire le responsabilità all’interno di un’azienda; altri ancora leggono con entusiasmo il principio di *accountability* richiamato dal GDPR (tradotto con “responsabilizzazione”), peraltro citato solo una volta e con riferimento al solo titolare.

È necessario ricordare che tutte le organizzazioni prevedono una distribuzione di responsabilità interne, anche se queste non comportano designazioni a norma di qualche legge. Le norme ISO sono molto chiare in proposito: prevedono che siano assegnati ruoli, responsabilità e poteri, secondo quanto necessario. Tutti questi ruoli, responsabilità e poteri sono poi soggetti a verifiche periodiche, in modo da verificare l’efficacia della soluzione identificata.

Audit interni ed esterni

La versione italiana del GDPR usa molti termini diversi per tradurre “audit”. Le verifiche richieste dal GDPR devono essere comunque viste come meccanismi di miglioramento: non devono colpevolizzare singole persone, bensì identificare carenze di processo per trovare la migliore soluzione.

Quando un audit identifica delle carenze, la soluzione può richiedere la modifica di uno o più processi, che deve essere apportata il più tempestivamente possibile. Tale modifica può comportare anche quella di regolamenti e procedure e questo è uno dei motivi per cui la distribuzione degli aggiornamenti deve essere efficiente: in caso contrario ci sarà eccessiva resistenza al cambiamento.

Conclusioni

La scelta di metodi efficaci ed efficienti per gestire gli adempimenti previsti dal GDPR è

fondamentale. Un metodo inefficiente diventa in poco tempo inefficace. Inutile pianificare un processo rigorosissimo, se poi non viene seguito. Meglio adottare un processo in apparenza meno rigoroso, ma che si integra nelle attività aziendali e sia mantenuto nel tempo.

Anche in queste scelte vede la propria applicazione il principio di *privacy-by-design*: fin dalla progettazione dei processi è necessario chiedersi se potranno essere mantenuti nel tempo con le risorse a disposizione e come è possibile bilanciare il rigore con l'efficienza.

A cura di: **Cesare Gallotti**