Verifica dell’accountability e compliance nell’Indagine internazionale “Privacy Sweep 2018”

Author : Sergio Guida

Date : 7 Maggio 2019

Regioni, Province autonome e società controllate devono ancora impegnarsi per il pieno rispetto del principio di responsabilizzazione.

Le imprese e gli enti pubblici analizzati dalle Autorità per la protezione dei dati personali di 18 Paesi - inclusa l’Italia - mostrano generalmente di aver ben compreso i concetti base del **principio di accountability**. Tuttavia, permangono **criticità** significative rispetto all’implementazione di politiche e programmi specifici a tutela della privacy.

Avviata lo scorso settembre, *Privacy Sweep 2018* è **un'indagine a carattere internazionale** dedicata al principio di **responsabilizzazione (*accountability*)** sancito dal Regolamento Ue 2016/679 sulla protezione dei dati personali e prende in esame le misure che titolari o responsabili del trattamento hanno adottato per garantire e dimostrare il rispetto delle norme e degli standard in materia di GDPR.

Altre 17 Autorità garanti della privacy di altrettanti Paesi del mondo, oltre all’Autorità italiana, hanno partecipato all'indagine sull'*accountability* che fa seguito ad analoghe indagini effettuate negli scorsi anni riguardo alle **informative privacy** su siti web e le app per la telefonia mobile, ai servizi online destinati a minori, all’Internet delle cose.

Ogni Autorità coinvolta ha scelto autonomamente lo specifico settore di analisi, dal turismo alla salute, dalla pubblica amministrazione alle telecomunicazioni. Il **Garante italiano** ha concentrato la sua azione sulle Regioni e sulle Province autonome, estendendo il campo anche alle rispettive società controllate, in considerazione della quantità e della rilevanza dei trattamenti di dati personali da queste effettuate per lo svolgimento di compiti di interesse pubblico. Si tratta di un campione che copre oltre un quinto delle 356 organizzazioni oggetto dell’indagine internazionale.

L'iniziativa è coordinata dalla *Global Privacy Enforcement Network* **(GPEN)**,ovvero la Rete globale per l'applicazione delle norme in materia di privacy, che ad oggi comprende più di 60

Autorità Garanti nel mondo ed è stato costituito nel 2010 a seguito di una raccomandazione dell'OCSE. Il suo obiettivo è quello di promuovere la **cooperazione internazionale fra le Autorità di controllo** per la privacy, vista la crescente globalizzazione dei mercati e l'esigenza delle imprese e dei consumatori di disporre di un flusso di informazioni personali senza soluzioni di continuità, indipendentemente dai confini nazionali. La rete, che ha natura informale, comprende oltre 60 autorità di 39 paesi.

La lettura dei risultati della *Sweep 2018* circa le modalità individuate dai titolari del trattamento per garantire in modo responsabile la conformità alle norme di protezione dei dati consente di rilevare importanti **esempi di "buone pratiche"** che delineano un percorso destinato al progressivo miglioramento nelle misure a tutela della privacy adottate dagli enti pubblici. Tuttavia emerge un **quadro ancora non soddisfacente**, dal momento che sono ancora molti i casi in cui non risultano essere previsti processi dedicati alla trattazione delle richieste degli interessati; come pure sono risultati carenti i sistemi di gestione dei reclami e, carenza ancora più rilevante, non risultano ancora pienamente adeguati i meccanismi di prevenzione e contrasto di eventuali violazioni alla sicurezza ai dati.

Il responsabile dell'intelligence di ICO (*Information Commissioner's Office*, cioè l'Autorità Garante nel Regno Unito), Adam Stevens, ha dichiarato: *"I risultati suggeriscono che mentre le organizzazioni internazionali contattate hanno una buona comprensione del concetto di base della responsabilità, nella pratica vi è un significativo margine di miglioramento*. *È importante che le organizzazioni dispongano di adeguate misure tecniche e organizzative. Ciò include l'adozione di chiare politiche di protezione dei dati, l'adozione di un approccio di 'data protection by design and default' e il continuo controllo e monitoraggio delle prestazioni e del rispetto delle norme e dei regolamenti sulla protezione dei dati".*

I membri GPEN partecipanti hanno preso contatto con 356 organizzazioni in 18 paesi durante lo "*sweep*" e hanno raggiunto le seguenti **conclusioni:**

- Quando si tratta di monitorare le prestazioni interne in relazione agli standard di protezione dei dati, molte organizzazioni sono risultate inadeguate, con circa un quarto che ha risposto di non avere programmi in atto per condurre autovalutazioni e/o audit interni.
- Le organizzazioni si sono rivelate generalmente abbastanza brave nel fornire formazione per la protezione dei dati al personale, ma spesso non hanno fornito formazione di aggiornamento al personale esistente.
- Le organizzazioni che hanno indicato di avere in atto programmi di monitoraggio hanno generalmente fornito esempi di buone pratiche, osservando che conducono audit annuali o revisioni e / o autovalutazioni regolari.
- Quasi tre quarti delle organizzazioni di tutti i settori e giurisdizioni hanno nominato un individuo o una squadra che si assumerebbe la responsabilità di garantire che la propria organizzazione rispettasse le norme e i regolamenti in materia di protezione dei dati.
- Oltre la metà delle organizzazioni intervistate ha dichiarato di avere documentato procedure di risposta agli incidenti e di mantenere aggiornati i record di tutti gli incidenti e le violazioni della sicurezza dei dati. Tuttavia, un certo numero di organizzazioni ha dichiarato di non avere processi in atto per rispondere in modo appropriato in caso di un

incidente di sicurezza dei dati.

A seguito dell'indagine, i singoli membri di GPEN possono contattare le organizzazioni dei propri Paesi per valutare quali azioni correttive devono intraprendere per migliorare i controlli degli utenti sulle loro informazioni personali.

La sintesi dei risultati italiani

19 soggetti pubblici (Regioni e Provincie autonome) e 54 società *in-house* analizzate.

1. **Governance della privacy**
   Il 20% delle Regioni non ha adottato una procedura interna per la gestione dei dati personali nell'organizzazione o non la applica correttamente nelle attività quotidiane. La maggior parte delle Regioni hanno incaricato una o più persone competenti in materia di *governance* e gestione della protezione dei dati personali, a un livello gerarchico sufficientemente elevato nell'organizzazione.
2. **Formazione, monitoraggio e consapevolezza**
   La maggior parte delle regioni e delle società *in-house* prestano dovuta attenzione a un'adeguata formazione dei dipendenti in materia di protezione dei dati personali. Tuttavia, nel 40% dei casi non risulta essere monitorato il livello di attuazione delle pratiche corrette per un adeguato trattamento dei dati.
3. **Trasparenza**
   Il livello di trasparenza nel trattamento dei dati risulta adeguato, per merito di specifiche informative rese disponibili agli interessati al trattamento dei dati personali. Emerge che esse sono di norma costantemente aggiornate e facilmente accessibili; in pochi casi i soggetti sottoposti all'analisi sono risultati eccessivamente sintetici nel presentare l'informativa e in alcuni di questi casi viene proposta la sola *privacy policy* del sito web.
4. **Capacità di risposta e gestione degli incidenti di sicurezza**
   L'aspetto più critico risiede nella circostanza che ben il 24% delle società e il 48% delle Regioni non abbiano definito policy e procedure per la gestione delle richieste e dei reclami da parte degli interessati, o delle stesse Autorità. Viene sottolineato, altresì, il deficit delle misure adeguate per la gestione dei *Data Breach*: il 20% delle organizzazioni non ha implementato una procedura di risposta agli incidenti di sicurezza che includa, peraltro, la notifica all'Autorità e, in caso di alto rischio per le libertà e i diritti degli interessati, anche la comunicazione a questi ultimi. Preoccupa anche il dato secondo cui il 25% delle organizzazioni parrebbe non disporre di un registro per documentare le violazioni subite.
5. **Valutazione e monitoraggio dei rischi**
   Il 24% delle società *in-house* e – addirittura - il 58% delle Regioni non hanno documentato processi per la valutazione dei rischi sulla protezione dei dati personali (DPIA) in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi.
   Tuttavia, la maggior parte dei soggetti analizzati dispone di un registro dei trattamenti effettuati. Il 20% delle Regioni dovrebbe invece implementare misure adeguate alla conservazione e la tracciabilità dei dati personali comunicati o trasmessi a terzi.

Antonello Soro, presidente dell'**Authority italiana**, ha dichiarato che *"il nuovo Regolamento Ue*

in materia di privacy ha valorizzato in maniera determinante la 'funzione sociale' della protezione dei dati personali, attribuendo un ruolo chiave e una più marcata responsabilità ad aziende e pubbliche amministrazioni. *I risultati dello Sweep 2018 confermano che c'è ancora molto da fare – sia in Italia, sia all'estero - affinché i principi a tutela della privacy vengano declinati correttamente nelle pratiche quotidiane, nei processi organizzativi e lungo tutta la catena decisionale nel settore pubblico e in quello privato".*

Il Garante ha aggiunto che *"la nostra Autorità continuerà a svolgere, con la massima attenzione, le proprie funzioni di controllo e correttive, nonché di promozione della consapevolezza del valore dei dati"*.

Certo, **la *data awareness* è uno dei presupposti basilari**. Perciò, se è vero che gli utenti e prima ancora gli individui (le "*natural persons*") sono al contempo il centro e il *target* della disciplina UE in materia di protezione dei dati, non meno rilevante appare il ruolo di enti e organismi pubblici che gestiscono, ancor prima dei servizi, i dati dei cittadini.

E che, come si è visto, hanno ancora molto da impegnarsi.

Articolo a cura di **Sergio Guida**