GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Indagine internazionale sul rispetto della privacy - Sweep 2018. Garante privacy: Regioni, Province autonome e società controllate devono ancora impegnarsi per il pieno rispetto del principio di responsabilizzazione (accountability)

Indagine internazionale sul rispetto della privacy - Sweep 2018
Garante privacy: Regioni, Province autonome e società controllate devono ancora impegnarsi per il pieno rispetto del principio di responsabilizzazione (accountability)

Nonostante la maggior parte delle imprese e degli enti pubblici analizzati dalle Autorità per la protezione dei dati personali di 18 Paesi - inclusa quella italiana - mostri una buona comprensione dei concetti base del principio di responsabilizzazione (accountability), permangono carenze significative in merito alla concreta attuazione di politiche e programmi specifici a tutela della privacy.

E' quanto emerge dall'indagine a tappeto ("sweep"), a carattere internazionale, avviata lo scorso settembre dalle Autorità per la protezione dei dati personali appartenenti al Global Privacy Enforcement Network (GPEN) per verificare il rispetto del principio di accountability, introdotto anche in Europa dal GDPR, con il Regolamento Ue sulla protezione dei dati.

Ogni Autorità coinvolta ha scelto autonomamente lo specifico settore di analisi, dal turismo alla salute, dalla pubblica amministrazione alle telecomunicazioni. Il Garante per la privacy italiano ha analizzato Regioni e Province autonome, nonché le rispettive società controllate che effettuano rilevanti trattamenti di dati personali per lo svolgimento di compiti di interesse pubblico, coprendo oltre un quinto delle 356 organizzazioni oggetto di “sweep” in tutto il mondo.

Le risultanze raccolte dagli esperti delle diciotto Autorità, sulle modalità individuate dai titolari del trattamento per garantire in modo responsabile la conformità alle norme di protezione dei dati, hanno fatto emergere un quadro ancora non soddisfacente. Pur rilevando esempi di buone prassi, si è osservato, ad esempio, che in molti casi non erano previsti processi specificamente dedicati alla trattazione di reclami o alle richieste degli interessati, né meccanismi idonei a gestire adeguatamente eventuali violazioni alla sicurezza ai dati. Il Garante italiano ha comunque rilevato nel nostro Paese, anche a seguito dell’analisi avviata, un progressivo miglioramento nelle misure a tutela della privacy adottate dagli enti pubblici.

“Il nuovo Regolamento Ue in materia di privacy - dichiara il Presidente Antonello Soro - 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.

La nostra Autorità - sottolinea il Presidente Soro - continuerà a svolgere, con la massima attenzione, le proprie funzioni di controllo e correttive, nonché di promozione della consapevolezza del valore dei dati”.

Roma, 5 marzo 2019

SINTESI DEI RISULTATI ITALIANI

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

1. Governance della privacy

Un quinto delle regioni non ha ancora adottato una procedura interna per la gestione dei dati personali nell'organizzazione o non l'ha applicata correttamente nelle attività quotidiane. Quasi tutte, però, 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 riconoscono l'importanza di un'adeguata formazione dei dipendenti in materia di protezione dei dati personali. Nel 40% dei casi, però, le organizzazioni non hanno posto in essere alcun monitoraggio in merito all'attuazione di corrette pratiche nel trattamento dei dati personali.

3. Trasparenza

E' garantita un'adeguata trasparenza nel trattamento dei dati, attraverso specifiche informative agli interessati sul trattamento dei dati personali. Tali informative, di solito, sono costantemente aggiornate e facilmente accessibili, sebbene alcune organizzazioni appaiono limitarsi a presentare la sola privacy policy del sito web.

4. Capacità di risposta e gestione degli incidenti di sicurezza

Appare grave che 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.

Si evidenziano ancora carenze in merito alla gestione degli incidenti di sicurezza – i cosiddetti Data Breach – tanto che un quinto delle organizzazioni non ha ancora implementato una procedura di risposta agli incidenti di sicurezza che includa, tra l'altro, la notifica all'Autorità e, in caso di alto rischio per le libertà e i diritti degli interessati, anche la comunicazione a questi ultimi. Un quarto delle organizzazioni, inoltre, sembra non disporre di un registro per documentare le violazioni subite.

5. Valutazione e monitoraggio dei rischi

Il 24% delle società in-house, ma addirittura il 58% delle Regioni, non hanno processi documentati per la valutazione dei rischi sulla protezione dei dati personali (DPIA), in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi.

La maggior parte dei soggetti analizzati ha creato un registro dei trattamenti effettuati. Un quinto delle Regioni, però, dovrebbe fare uno sforzo maggiore per tenere traccia anche dei dati personali comunicati o trasmessi a terzi.

SINTESI DEI RISULTATI INTERNAZIONALI

356 soggetti pubblici e privati analizzati in 18 paesi.

- Quasi il 75% degli organismi contattati, a prescindere dal settore o dal paese di attività, hanno designato un responsabile o una unità incaricati di garantire il rispetto delle norme in materia di protezione dei dati.

- Mentre si pone grande attenzione alla formazione del personale in materia di protezione dei dati, spesso non si provvede a un aggiornamento di tale formazione.

- Circa un quarto degli organismi risultano privi di specifici programmi di autovalutazione o di monitoraggio interno delle norme in materia di protezione dei dati.

- Gli organismi che dispongono di programmi di monitoraggio interno segnalano in genere esempi di buone prassi, quali rilevamenti o indagini svolte con cadenza annuale e/o attività periodiche di autovalutazione.

- Oltre la metà dei soggetti presi in esame risulta disporre di procedure documentabili di risposta in caso di incidenti che riguardano la sicurezza dei dati, nonché di registrazioni aggiornate di tutti gli incidenti e le violazioni di sicurezza. Tuttavia,

molti organismi non hanno ancora procedure atte a rispondere adeguatamente a questi eventi.

Note

1. La Rete globale delle autorità incaricate di dare attuazione alle norme sulla privacy (Global Privacy Enforcement Network, GPEN) è stata creata nel 2010 su raccomandazione dell'OCSE. Mira a promuovere la cooperazione transfrontaliera fra le autorità per la privacy in un contesto sempre più globalizzato, in cui le attività commerciali e gli stessi consumatori necessitano di flussi ininterrotti di dati personali. I membri della Rete collaborano per potenziare la tutela della privacy in questo contesto globale. La rete, che ha natura informale, comprende oltre 60 autorità di 39 paesi.

2. Le attività di "sweep" della rete GPEN sono attualmente coordinate dall'Information Commissioner del Regno Unito e dall'Office of the Privacy Commissioner della Nuova Zelanda.

3. Per questo sweep, sono stati elaborati questionari che le autorità partecipanti hanno somministrato agli organismi presi in esame, con particolare riguardo agli elementi fondamentali di una gestione responsabile delle informazioni personali.