Poche le società pronte al test

Tre anni in un battito di ciglia e le statistiche ci dicono che non sono bastati. Né in Italia né in Europa.

Uno studio della società internazionale di consulenza Gartner rileva che solo 4 su 10 privacy manager ritengono le società di appartenenza preparate ad affrontare e governare il Regolamento Ue sulla protezione dei dati (fonte www.iapp.org), addebitando questa sfiducia, tra l'altro, alla volatilità di norme generiche.

Sul fronte internazionale anche la ricerca Sweep 2018 (fonte www.garanteprivacy.it) non offre un panorama ridente: circa un quarto degli organismi interrogati (356 soggetti pubblici e privati analizzati in 18 paesi) risulta privo di specifici programmi di autovalutazione o di monitoraggio interno delle norme in materia di protezione dei dati; 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. Peraltro quasi il 75% degli organismi coinvolti, a prescindere dal settore o dal paese di attività, ha designato un responsabile o una unità incaricati di garantire il rispetto delle norme in materia di protezione dei dati.

A livello italiano, le notizie sono sulla stessa lunghezza d'onda.

Uno studio condotto dall'Osservatorio di Federprivacy su ben 3 mila siti dei comuni italiani, tra le varie non conformità e altre carenze riscontrate, ha rivelato che 1.435 di essi (47%) continuano a utilizzare connessioni non sicure basate sul vecchio protocollo «http», e per questo sono etichettati come «non sicuri» dai principali browser. Inoltre, 1.079 siti di comuni (36%) non rendono disponibili i dati di contatto del Responsabile della protezione dei dati (il Dpo, data protection officer), figura obbligatoria per tutte le pubbliche amministrazioni.

E, anche, in specifici settori, si evidenzia che il percorso è ancora lungo.

Per esempio uno studio condotto da Symantec su oltre 45 siti web, che gestiscono attivamente le prenotazioni di più di 1.500 hotel, ha rilevato che il 67% dei loro siti internet per le prenotazioni ha involontariamente perso i dati personali degli ospiti.

Gli hotel coinvolti nello studio si trovano distribuiti in 54 paesi tra cui gli Stati Uniti, il Canada e molte nazioni dell'Unione europea.

La doppia faccia dell'accountability

La parola magica della privacy europea è «accountability», ma è un'arma a doppio taglio. Il regolamento Ue 2016/679, si dice, ha responsabilizzato le imprese, sburocratizzando la privacy. Così da un lato non bisogna più mandare una notificazione del trattamento al Garante della privacy, non bisogna più chiedere una verifica preliminare per i trattamenti più rischiosi, si deve costruire la sicurezza informativa e non-informatica senza dovere sottostare a una griglia predeterminata: sono tutti aspetti che evocano possibilità di autoregolamentazione, di autodeterminazione, di maggiore libertà. Ma dall'altro lato non c'è una definizione esatta di tutta una serie di parametri, per cui alla domanda «siamo a posto?» non si può più rispondere «sì, perché abbiamo fatto gli adempimenti esattamente descritti da una norma». Questo perché non ci sono norme che descrivono esattamente gli adempimenti, ma questi devono essere «valutati» nella loro conformità al Gdpr, e cioè bisogna stimare se si sono raggiunti i risultati, ma la stima è sempre un po' approssimativa.

In questo quadro, facile constatare che tutto dipende dal valutatore. E chi è il valutatore nei singoli casi? Innanzi tutto il cosiddetto titolare del trattamento, che deve valutare se, come e quanto mettersi a posto: il suo problema è economico e organizzativo, e cioè quanto mi costa mettermi a posto e come deve cambiare il mio modo di lavorare? Ma poi c'è l'autorità di controllo, che dovrà costruire una serie di parametri per stimare, senza disparità di trattamento, la conformità al Gdpr e dare prescrizioni concrete.

Ma non basta perché c'è la magistratura, che deve vagliare i provvedimenti dell'autorità di controllo. E si ricordi che stiamo parlando, a seconda delle competenze, di Garanti nazionali ed europei e, quindi, di giudici italiani ed europei. Questo significa che, in questo momento storico, per arrivare a una regola semi-certa su problemi specifici bisognerà attendere l'opinione dell'ultimo valutatore sul singolo caso: qualche cavia dovrà fare la sua tragica parte.

ATTIVITÀ DI ADEGUAMENTO AL REGOLAMENTO 2016/679

ADEMPIMENTI	ART. RGPD	DOCUMENTI DA PRODURRE	AZIONI
Nomina autorizzati	29	Nomina dipendenti e collaboratori	Mappatura delle posizioni di soggetti interni che trattano dati
			Verifica e aggiornamento della profilazione del personale interno
			Mappatura delle nomine a «incaricato del trattamento» precedenti al RGPD
			Eventuale integrazione atti di nomina precedenti al RGPD
			Stesura nuovi atti di nomina ad «autorizzato al trattamento»
Formazione autorizzati	39	Corsi per gli autorizzati	Corsi base per autorizzati al trattamento
			Corsi per livelli apicali
			Corsi per RPD/DPO
			Corsi specialistici per settori particolari (media, IT ecc.)
Rapporti con interessati	12, 13, 14	atti di informazione	Verifica atti di informazione esistenti
			Adeguamento atti di informazione ai nuovi contenuti
			Eventuale abbinamento atti di informazione a icone
			Istituzione ufficio per risposte alle richieste degli interessati
			Protocollo delle attività dell'ufficio «trasparenza»
	6, 7, 8, 9	Raccolta consensi	Verifica necessità del consenso
			Predisposizione formule in linea con RGPD
			Verifica consensi precedenti al RGPD
			Adeguamento «vecchi» consensi
			Cautele particolari in caso di minori di età (servizi della società dell'informazione)
			Procedure per la gestione delle revoche del consenso
	6, 9	Condizioni di liceità diverse dal consenso	Verifica condizioni di liceità diverse dal consenso
			Predisposizione cautele in linea con RGPD
			Verifica cautele precedenti al RGPD
			Adeguamento «vecchie» cautele
RPD/DPO	37, 38, 39	Nomina RPD/DPO	Verifica obbligo/opportunità nomina
			Scelta tra dipendente oppure professionista/organizzazione esterna
			Stesura e sottoscrizione atto di designazione/contratto
			Comunicazione al Garante di avvenuta nomina del RPD/DPO
			Esecuzione misure previste nel contratto
			Istituzione di ufficio del RPD/DPO
			Istituzione di punto di contatto del RPD/DPO con interessati