impresacity

Mensile

MERIDIAN COMMUNICATIONS

Data 12-2017
Pagina 48/49
Foglio 1 / 2

Gdpr, la scommessa italiana

Il nuovo regolamento europeo sulla privacy, che entrerà in vigore dal 25 maggio 2018, porterà con sé numerosi cambiamenti e obblighi per le imprese. Le realtà del nostro Paese faticano però a creare cultura interna e rischiano di rimanere indietro

di **Alessandro Andriolo**

Il tempo stringe. Il prossimo 25 maggio entrerà in vigore anche in Italia il General Data Protection Regulation, noto con la sigla Gdpr: un regolamento adottato a livello europeo che impone alle aziende operanti nei Paesi membri della Ue una serie di novità di assoluto rilievo in materia di trattamento dei dati personali. Il Gdpr integra di fatto l'attuale Codice della Privacy, introdotto in Italia con il decreto legislativo 196/2003, e attualizza la Direttiva 95/46/Ce, non più adatta a garantire un trattamento trasparente delle informazioni nell'era di Internet e dei Big Data. Le novità più rilevanti del regolamento europeo sono numerose. Innanzitutto, il legislatore ha voluto ampliare l'orizzonte territoriale, applicando il Gdpr sia nel caso in cui l'azienda o il cosiddetto data subject risiedano nell'Unione, ma anche quando un'organizzazione extra-Ue tratta le informazioni dei residenti europei. È il caso, ad esempio, dei colossi hi-tech statunitensi (anche se i contratti siglati prima dell'entrata in vigore del Gdpr non verranno toccati dalle nuove norme).

In secondo luogo, gli utenti potranno contare sia sul diritto di accesso ai propri dati, sia sul diritto all'oblio (già in vigore dal 2014), ma anche sulla possibilità di revocare il consenso a determinati trattamenti. Uno degli aspetti più interessanti del regolamento è l'introduzione di sanzioni pecuniarie decisamente elevate. Le imprese che non dimostrano piena compliance ai principi base del Gdpr rischiano multe fino a 20 milioni di euro o per un massimo del 4 per cento del fatturato annuo.

"Bruxelles ha comunque lasciato agli Stati membri il compito di disciplinare le regole e l'effettiva applicazione delle sanzioni amministrative", ha spiegato l'avvocato Valentina Frediani, fondatore e Ceo dello studio Colin & Partners, durante un evento incentrato sul Gdpr organizzato da Sb Italia nel campus milanese di Data4. Il terzo punto fondamentale dell'impianto è il concetto di data protection by design and by default, due principi che devono obbligatoriamente andare a braccetto.

Cosa significa? "Che tutti i nuovi prodotti e servizi devono garantire, fin dalla loro progettazione, una privacy assoluta grazie a concetti come la pseudonimizzazione, la minimizzazione, la data retention, la sicurezza end-to-end per tutto il ciclo di vita dell'informazione e così via", ha aggiunto Frediani. In particolare, due aspetti che possono sembrare nuove alle orecchie delle aziende sono la pseudonimizzazione e la minimizzazione.

Nel primo caso si parla di un procedimento attraverso cui le informazioni di profilazione vengono conservate in una forma tale da impedire l'identificazione dell'utente, grazie al ricorso al mascheramento e ai tag; mentre la minimizzazione garantisce che le organizzazioni trattino di default soltanto i dati personali necessari per ogni specifica finalità del trattamento. In sintesi, le impre-

se non possono superare quanto espressamente previsto.

Ma il Gdpr nasce non solo per assicurare una maggiore privacy ai cittadini del Vecchio Continente, ma anche per garantire loro più sicurezza. Un capitolo centrale del testo approvato da Bruxelles riguarda i data breach, vale a dire le violazioni nei sistemi delle organizzazioni che portano alla fuoriuscita di informazioni. Dal 25 maggio 2018 le realtà che subiscono attacchi di questo genere avranno l'obbligo di comunicare eventuali perdite al Garante e, in casi rilevanti, anche ai diretti interessati.

E le imprese coinvolte in data breach sono sempre di più. Negli ultimi 12 mesi sono stati trafugati ben due miliardi di record, con un caso di furto riuscito in oltre un attacco su due. Si parla di credenziali di accesso ai servizi, di dati personali (tra cui quelli finanziari), di informazioni riservate delle aziende e molto altro. Secondo la Sans 2017 Data Protection Survey, un'organizzazione su due ha dovuto fronteggiare almeno un ransomware, quasi una su tre una minaccia interna e oltre una su dieci la manomissione di informazioni.

"I data breach impattano soprattutto sulla fiducia dei clienti, sulla reputazione del brand e a livello legale", ha sottolineato Elena Vaciago, associate research manager di The Innovation Group (Tig). Ecco quindi che diventa fondamentale per le società agire in modo da rispettare i principi del Gdpr. Ma cosa stanno facendo di concreto le aziende per adeguarsi al regolamento?

"In questa fase l'attività più frequente tra le imprese sembra essere l'inventario dei dati degli utenti, citato dal 49 per cento delle organizzazioni", ha commentato Vaciago citando un'indagine di Crowd Research Partners. "Il 31 per cento delle aziende, invece, sta riprogettando applicazioni e database per abilitare la data protection by default, mentre il 28 per cento di loro sta procedendo ad audit interni per scovare record isolati contenenti informazioni sensibili".

Ma, in generale, le imprese italiane sembrano essere ancora indietro. È proprio un'indagine di autovalutazione promossa da Sb Italia a testimoniarlo. Sul tema dell'awareness quasi un'organizzazione su tre ammette di non promuovere la cultura interna e il 43 per cento dichiara di non aver ancora previsto revisioni periodiche della compliance al Gdpr. Va meglio sul fronte del trattamento dei dati, con il 65 per cento che dice di sapere almeno in parte quali sono le informazioni in uso (e da dove provegono) e con sei aziende su dieci che hanno aggiornato le procedure per ottenere il consenso degli utenti.

Non a caso, secondo la Cyber Risk Management Survey 2017, l'area meno critica per l'adeguamento al Gdpr è rappresentata dalla componente "informativa e consensi", mentre il problema maggiore è costituito dall'introduzione nel team del cosiddetto data protection officer (Dpo). Figura centrale del regolamento, il Dpo diventerà il responsabile della protezione delle informazioni e non potrà essere in alcun modo l'It manager. Il Gdpr prevede chiaramente che questo nuovo ruolo dovrà essere terzo e indipendente e dovrà riportare direttamente ai vertici.

È chiaro quindi come il Gdpr, pur dando maggiori diritti ai cittadini, rappresenti un onere non indifferente per le imprese, anche dal punto di vista tecnologico. Per garantire principi come portabilità, correzione o cancellazione immediata dei dati sono infatti necessarie soluzioni capaci di reperire velocemente le informazioni e di esporle in formati aperti, compatibili con tutti gli strumenti presenti sul mercato.

L'unica strada percorribile sembra essere quella di un'automatizzazione "estrema" delle attività di gestione dei dati, indirizzandosi verso repository centralizzati e, soprattutto, molto sicuri. La via del cloud sarà, in molte situazioni, un tragitto obbligato in particolar modo per le piccole e medie imprese.

"L'importante è avvalersi di un partner con una comprovata esperienza", commenta Massimo Casaletta, business development manager It Service Management di Sb Italia. "Abbiamo sviluppato internamente una metodologia ad hoc per aiutare i nostri clienti nel viaggio verso il Gdpr. Un processo che si struttura in tre fasi (consulenza, implementazione e governance, ndr) per adeguarsi al nuovo regolamento. Un approccio personalizzato e su misura, aperto alla collaborazione con partner tecnologici come Fortinet, Rsa e Commvault, che garantisce soluzioni modulari e flessibili, oltre a competenze certificate in ambito applicativo e infrastrutturale". ■

> Quasi un'organizzazione su tre non promuove la cultura interna e il 43 per cento dichiara di non aver ancora previsto revisioni periodiche della compliance al Gdpr