Data Protection Officer, per una governance del GDPR

Il nuovo regolamento della Privacy stabilisce la presenza di un responsabile della protezione delle informazioni, funzione che non potrà essere più delegata all'IT manager

Il General Data Protection Regulation (**Gdpr**) entrerà in vigore a maggio 2018 ed è stato pensato per uniformare la **protezione dei dati all'interno dell'Unione Europea**. Il Gdpr regola anche l'esportazione dei dati personali al di fuori dell'Unione Europea e per questo motivo le sue implicazioni saranno globali e significative per tutte le aziende internazionali.

Il Gdpr andrà ad integrare il Codice della Privacy, introdotto in Italia con il decreto legislativo 196/2003, attualizzando 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**.

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".*

Pubblicato il: 16/10/2017