Veneziepost.it URL: http://www.veneziepost.it/regolamento-privacy-ue-6792016-si-attua-ladeguamento-organizzativo/

05 marzo 2017

ADACTA RISPONDE

Regolamento Privacy UE 679/2016: come si attua l'adeguamento organizzativo?

Luca De Muri

Domenica 5 Marzo 2017 14:00

Quali sono le novità principali del nuovo Regolamento Privacy e quali sono le metodologie più opportune per poter sfruttare in azienda l'occasione per assicurarci maggiore efficienza? Sentiamo parlare di analisi dei rischi e modelli di gestione "strutturati e continui": cosa significa in concreto? Quali sono i rischi se ritardiamo o non svolgiamo le azioni necessarie?

Il Reg. UE 679/2016 introduce dal 25 maggio 2018 nei 28 Stati membri una medesima disciplina privacy uniforme. La sua diretta applicazione senza necessità di leggi di recepimento nazionali renderà di immediata applicazione varie novità da non sottostimare, a pena di sanzioni fino a decine di milioni di euro e, per le imprese, fino al 4% del fatturato di gruppo.

I dati personali oggetto di tutela legale sono trattati soprattutto, ma non solo, dalle funzioni aziendali IT, Human Resources e Sales/Marketing, Acquisti, Sicurezza/Ambiente chiamate quindi ad uno sforzo di ri-mappatura dei processi e delle modalità di trattamento (dipendenti dalla sempre più spinta multicanalità). Le società più esposte al rischio privacy sono innanzitutto quelle che offrono beni e servizi alle persone fisiche, ma ogni azienda ha dipendenti e altre figure coinvolte negli adempimenti. Alcune aziende dovranno nominare un Data Privacy Officer indipendente.

05 marzo 2017

Nuovi diritti quali il diritto alla portabilità del dato e il diritto alla comunicazione dei cd. data breach, impongono un'integrazione delle procedure ed un loro coordinamento con gli strumenti di gestione software e cyber-security. Va inoltre aggiornato il Documento Programmatico sulla Sicurezza (per molti fermatosi al 2011).

In passato l'attenzione si concentrava su inventari a vario livello (es. hardware, software, banche dati, ruoli), oggi tutto questo è solo il punto di partenza per un ragionamento che deve includere l'intera organizzazione. La privacy, dice il regolamento, deve essere adempiuta nativamente (by design) quindi va pensata già nel momento in cui ogni iniziativa e riorganizzazione viene introdotta in azienda, e non dopo. La privacy va altresì gestita "by default" e cioè adottando ari vari livelli tecniche che minimizzino i trattamenti limitandoli di volta in volta a quanto strettamente necessario ("need-to-know") e che all'interno dei trattamenti consentiti includano solamente i dati in chiaro indispensabili.

La privacy è anche "accountability": vale a dire puntuale responsabilizzazione e documentazione di quanto implementato. Non basta fare, occorre dimostrare. La privacy è un approccio risk-based e il relativo modello deve risultare efficace in concreto, pertanto occorre che l'azienda individui il proprio status organizzativo e costruisca gli adempimenti a partire dallo stesso. Ogni soluzione non tailor-made, pertanto, va valutata con estrema prudenza, così come va evitato di causare inopportuni "silos" tra diversi modelli di compliance ai diversi livelli (gestione qualità, modelli organizzativi 231): gli stessi vanno invece armonizzati. Le linee guida introdotte a livello nazionale in materia di sicurezza ICT, es. quelle dell'Agenzia Italia Digitale 26.4.2016 per la PA o l'Italian Cyber Security Report 2015 del Cyber Security National Lab possono costituire un punto di partenza, da sviluppare, ricordando sempre che la privacy non è solo informatica ma anche gestione di molte attività non ICT. La metodica preferibile è quella Quick-Win: ogni misura adottata deve creare un upgrade sostanziale e sempre misurabile nella riduzione del rischio privacy. La scadenza di legge è vicina ed una pianificazione tempestiva rientra nei doveri degli amministratori.

l.demuri@adacta.it