Tra meno di due mesi entrerà in vigore il nuovo regolamento europeo sulla tutela dei dati personali e della privacy. Occorre esserne informati e provvedere in tempo.

É l'ora del GDPR: siete preparati?

Dal 25 maggio 2018 entrerà in vigore il Regolamento Generale sulla Protezione dei Dati (GDPR – General Data Protection Regulation). Il GDPR stabilisce nuovi doveri e nuove responsabilità per i titolari e i responsabili del trattamento di dati personali. L'attuazione del GDPR toccherà tutte le organizzazioni che trattano dati personali nell'ambito della UE – indipendentemente dalla sede aziendale - e i suoi cittadini. Le imprese, soprattutto quelle di grosse dimensioni, si stanno trasformando in "data company". Di conseguenza, la corretta gestione del flusso informativo è diventata di vitale importanza a livello produttivo e competitivo.

Durante il convegno del 26 marzo 2018, organizzato da The Ruling Companies, manager ed esperti di questa che è divenuta ormai una materia fondamentale hanno spiegato cosa le aziende devono sapere al riguardo e come devono prepararsi per affrontare la "nuova privacy".

L'avvocato Paola Pucci (Partner, Studio Toffoletto De Luca Tamajo e Soci) ha sottolineato che innanzitutto è necessario innalzare il livello di attenzione e di preparazione in vista di questa scadenza. L'obiettivo della nuova regolamentazione non è ostacolare il business ma di favorirlo, elevando gli standard e garantendo maggior efficienza, qualità e competitività. I recenti fatti accaduti a Facebook dimostrano come un processo scorretto di immagazzinamento, analisi e distribuzione dei dati possa portare a danni concreti, a una perdita di credibilità e a un netto peggioramento dei risultati di business. Una gestione responsabile e trasparente dei dati è fondamentale per fidelizzare i clienti e competere nel mercato.

Il nuovo regolamento prevede sanzioni più elevate (fino al 4% del fatturato mondiale) in caso di gestione scorretta e obbliga alla denuncia in caso di violazione o smarrimento dei dati (data breach). Il GDPR si basa su diversi principi riguardanti il trattamento dei dati; oltre a quelli di liceità, adeguatezza e necessità, sono ritenute rilevanti la precisione e la trasparenza. Le aziende potranno utilizzare i dati solo per le finalità dichiarate nell'informativa. Ogni azienda dovrà essere in grado di dimostrare di aver adottato misure adeguate nell'ambito della gestione del proprio sistema informativo in relazione ai trattamenti svolti e di aver predisposto processi e procedure in grado di mantenere il livello di adeguatezza nel tempo. Inoltre, a partire dai singoli trattamenti, dovrà essere possibile documentare le misure di sicurezza adottate, IT e di business, e dimostrare i criteri in base ai quali tali misure possono essere considerate "adeguate".

L'avvocato Pucci ha citato alcuni dei punti chiave del regolamento: le aziende dovranno dichiarare con precisione il periodo di conservazione dei dati e il criterio con il quale è stato stabilito il relativo arco temporale. Inoltre, dovranno essere in grado di dimostrare come è stato ottenuto il consenso al trattamento dei dati e nominare una persona responsabile – adeguatamente formata – autorizzata al trattamento. Ogni organizzazione dovrà adottare le modalità più opportune per garantire

l'accountability nell'ambito della gestione dei sistemi informatici. Tutto il processo verrà seguito dal DPO (Data Protection Officer), la nuova figura professionale che supporterà le aziende nell'applicazione del regolamento e ne controllerà l'operato. Inoltre, il GDPR prevede maggiori tutele per il trasferimento dei dati fuori UE, soprattutto verso quei Paesi che non hanno standard adeguati in tema privacy.

Secondo Gabriele Faggioli (Responsabile Scientifico dell'Osservatorio Security & Privacy del Politecnico di Milano e Presidente del CLUSIT, l'Associazione Italiana Sicurezza Informatica) il tema della tutela della privacy è prima di tutto un fatto culturale e poi tecnico. L'incessante evoluzione tecnologica produrrà sempre più oggetti connessi, capaci di raccogliere ingenti quantità di dati e informazioni su abitudini e preferenze dei consumatori che spesso non si curano di tutelare la propria privacy. La spinta mediatica e la nuova legislazione aumenteranno il livello di attenzione e consapevolezza sia da parte degli utenti che dei decisori aziendali. L'approvazione del GDPR, comune a tutti gli Stati europei, è certamente un passo importante verso l'adeguamento delle practice aziendali.

Una ricerca svolta dal Politecnico di Milano su un campione di 160 aziende di grosse dimensioni ha rivelato che il 51% di esse sta già lavorando su progetti di adeguamento delle proprie policy sulla privacy, stanziando budget più elevati e di durata pluriennale (dal 2016 al 2017 gli investimenti in sicurezza informatica sono aumentati del 12%). Gli attacchi informatici sono in aumento e un numero crescente di organizzazioni sta denunciando di aver subito attacchi gravi.

Le grosse aziende - ma anche le PMI e la PA - dovranno attrezzarsi con piani di sicurezza dettagliati e adottare le misure più idonee a protezione dei dati personali. Per quanto riguarda la parte hard, i fornitori di tecnologia dovranno garantire "di default" la sicurezza dei sistemi.

Roberto Fermani (Responsabile Funzione Privacy, TIM) ha toccato nel suo intervento un altro aspetto fondamentale per le aziende, quello del data breach. Innanzitutto, secondo l'esperienza di Fermani, ogni impresa dovrebbe prevedere un piano scritto per la gestione degli incidenti di sicurezza che specifichi chiaramente "chi deve fare cosa" in caso di emergenza. Il secondo step consiste nel notificare al più presto la violazione al Garante in caso si abbia anche solo il sospetto di aver subito un attacco. Bisogna denunciare anche la distruzione di archivi oppure il furto o la perdita dei dispositivi contenenti dati dei propri clienti. Se informazioni sensibili, non cifrate, sono per qualsiasi ragione uscite dal controllo delle persone autorizzate al trattamento, l'azienda deve comunicarlo entro tre giorni anche ai soggetti lesi.

Nel caso in cui la gestione dei dati sia affidata a un fornitore esterno, l'azienda deve assicurarsi che le sue politiche siano corrette e conformi al regolamento. Consigliabile rivedere le condizioni contrattuali e predisporre delle tabelle per la valutazione del rischio.

Roberto Negro (Master Principal Solution Consultant Data Management, Data Quality & Governance, Oracle) sostiene che il trasferimento dei dati in cloud aumenti il livello di sicurezza e aiuti le imprese a semplificare la gestione. Oracle lavora sui temi del GDPR dal 2015 e ha modificato l'approccio aziendale alla sicurezza dei dati e alla tutela dei diritti dei soggetti. Oracle ha suddiviso il processo di gestione dei dati in quattro aree:

- Discovery: raccolta di informazioni sulla gestione attuale del dato.
- Enforcement: vengono rafforzati i livelli di sicurezza.
- Government&enrichment: si analizzano le misure di data governance e si integrano policy per garantire il rispetto dei diritti dei soggetti coinvolti.
- Foundation: si implementa il sistema di archivio e gestione dei dati coerente con il regolamento GDPR.

Nella visione di Igor Marcolongo (Head of Process & Compliance, Infocert) il data processing è questione di trust. Infocert, che di occupa di digital trust, opera in modo conforme alla normativa eIDAS (electronic IDentification, Authentication and trust Services) introdotta nel 2014 dall'UE per regolamentare l'identificazione elettronica e i trust services per le transazioni elettroniche nel Mercato europeo comune. La crittografia, nelle sue varie declinazioni - firma digitale, timestamp, digital identity - consente di certificare l'identità di una persona e validare documenti di diverso tipo. Questi strumenti hanno un ruolo fondamentale nell'aumentare il livello di affidabilità e nel proteggere chi li utilizza da spiacevoli frodi di varia natura.
Il GDPR si sposa perfettamente con il regolamento eIDAS: il primo garantisce ai cittadini maggiori tutele, mentre il secondo regola la gestione di strumenti che possono produrre documenti e identità digitali “certe” limitando i rischi.
Gli ambiti di applicazione di queste nuove normative sono davvero numerosi, ad esempio Infocert ha lavorato in campo sanitario per digitalizzare in modo sicuro le pratiche di una struttura pubblica che utilizzava solo informative cartacee.
Gli strumenti tecnologici a supporto esistono già da tempo, ma molte realtà non adottano misure idonee alla tutela della privacy. Ora il GDPR impone a tutti i soggetti di valutare e implementare le misure più adeguate per evitare i rischi legati al trattamento dei dati. Le aziende, a prescindere dalla propria dimensione, se hanno intenzione di operare all'interno dei confini UE, devono assicurare la migliore compliance rispetto alle nuove regole e garantire la tutela della privacy a dipendenti e clienti.

A cura della Redazione di Harvard Business Review Italia