Il Sole 24 ORE | Radiocor
Rapporti e Società
DICEMBRE 2017

Protezione dei dati. Per le aziende la parola d'ordine è prevenzione

Verso il nuovo Regolamento europeo con un approccio che responsabilizza direttamente le imprese

Conto alla rovescia verso l'applicazione del Regolamento europeo sulla protezione dei dati personali. Una trasformazione - spiega il Responsabile delle Relazioni Esterne e Media del Garante della Privacy, Baldo Meo - che assegna una diretta responsabilità al titolare del trattamento dei dati e che mette al centro il tema della prevenzione del rischio richiedendo un approccio sistemico delle imprese alla sicurezza dei dati.

Il 25 maggio 2018 diventerà pienamente applicabile il nuovo Regolamento. Quali sono le priorità a cui adeguarsi per una azienda?

Il nuovo Regolamento Ue dà vita a un quadro armonizzato di regole in grado di superare il disomogeneo recepimento della Direttiva 95/46 da parte degli Stati, ma soprattutto in grado di calare i principi fondamentali del

trattamento dei dati (necessità, proporzionalità, finalità, liceità) nel mondo digitale. L'intero tessuto normativo del nuovo Regolamento ha come obiettivo quello di adeguare la disciplina della protezione dei dati all'evoluzione tecnologica, sviluppando uno spazio di libertà e sicurezza, e, insieme, un clima di fiducia per lo sviluppo dell'economia digitale in tutto il mercato dell'Unione. Tra le numerose novità introdotte del Regolamento alcune sono destinate ad avere un particolare impatto. Si passa innanzitutto da un approccio di tipo formalistico - autorizzatorio a un sistema incentrato su una diretta e maggiore responsabilizzazione (accountability) dei titolari del trattamento come sono appunto le imprese. Assume quindi un'importanza fondamentale la prevenzione del rischio, con l'introduzione di istituti nuovi come la "valutazione d'impatto" per trattamenti di dati che presentino rischi elevati per i diritti e le libertà delle persone. Vengono rafforzati i diritti degli interessati e le misure di tutela. Le sanzioni si fanno pesanti fino a raggiungere il 4% del fatturato globale annuo.

Una innovazione essenziale è la figura del Responsabile della protezione dati (RPD), chiamato ad assolvere anche una funzione preventiva, orientando l'organizzazione aziendale verso modelli virtuosi dal punto di vista della protezione dati, sensibilizzando e formando il personale, sorvegliando sullo svolgimento della valutazione d'impatto, cooperando con l'Autorità Garante e fungendo da interfaccia per gli interessati che si rivolgano all'azienda per esercitare i propri diritti.

Considerata la rilevanza di tale figura ai fini della corretta attuazione del Regolamento, il Garante ne ha consigliato la designazione anche al di fuori dei casi di obbligatorietà (pubbliche amministrazioni e titolari che svolgano trattamenti di dati sensibili su larga scala o inerenti il controllo sistematico degli interessati).

>>> continua a pagina 3

«PUNTI DEBOLI? IN PRIMIS C'È L'ERRORE UMANO»

Il principale rischio per l'integrità dei dati? L'errore umano, l'interazione tra le persone che per incuria, poca conoscenza o dolo può originare seri problemi alla sicurezza dei dati. È questo il primo punto debole nella protezione dei dati sensibili e della privacy secondo Andrea Borghi, Responsabile Sicurezza Sistemi e Reti di Multipartner S.p.A.

>>> a pagina 4

INTEGRARE LA GESTIONE PRIVACY NEI SISTEMI ORGANIZZATIVI AZIENDALI

Il Responsabile della protezione dei dati è una delle innovazioni della GDPR, perno della organizzazione aziendale su privacy e sicurezza dei dati. Giovanni Libertini svolge questo incarico nel gruppo Filippetti, specializzato in System Integration e Management Services.

La GDPR mette al centro la figura del Responsabile della protezione dei dati personali (DPO). Come si organizza una azienda conforme al Regolamento?

Il GDPR stesso lascia intravedere il modus operandi: l'organizzazione deve governare la protezione dei dati personali mediante un "sistema di gestione privacy" che potrebbe basarsi su un approccio analogo allo standard definito nell'Annex SL, adottato in molte norme ISO come la 9001 e la 27001. Il sistema di gestione privacy dovrebbe integrarsi quanto più possibile nei sistemi di gestione o negli schemi organizzativi aziendali già esistenti. La figura del DPO, auspicabilmente rappresentato da un team multidisciplinare, garantendo l'interlocuzione con i vertici e la sorveglianza del rispetto della normativa, svolge di fatto anche il ruolo di auditor di prima e seconda parte di un sistema di gestione privacy.

>>> continua a pagina 2

>>> DALLA PRIMA PAGINA

METODOLOGIE STANDARD E SOFTWARE: GLI "ATTREZZI" DEL MESTIERE DEL DPO

GIOVANNI LIBERTINI (GRUPPO FILIPPETTI): "L'APPROCCIO PIÙ EFFICACE PER LA PROTEZIONE DEI DATI PARTE DALL'ADOZIONE DI METODOLOGIE STANDARD DI AUDIT E ANALISI DEL RISCHIO"

> IL RESPONSABILE DELLA PROTEZIONE DATI DEVE INTERLOQUIRE CON I VERTICI AZIENDALI E SORVEGLIARE IL RISPETTO DELLA NORMATIVA

Quale è la "cassetta degli attrezzi" del DPO: cioè quali sono gli strumenti tecnologici e non di cui non può fare a meno?

Posto che il DPO deve avere approfondita conoscenza della normativa e del contesto in cui opera l'organizzazione, occorre che adotti opportuni standard metodologici per svolgere la sua attività. In particolare, l'adozione di metodologie standard di audit e di analisi del rischio rappresenta l'approccio più corretto ed efficace. Gli attrezzi, quindi, sono le metodologie standard e gli strumenti tecnologici funzionali a porle in essere, come i GRC Tools (IT Governance, Risk and Compliance), sistemi software che razionalizzano la gestione dei rischi e i programmi di audit e consentono di mettere ordine alla sovrapposizione di norme alle quali un'organizzazione deve attenersi.

Ci sono accorgimenti particolari da utilizzare per proteggere i dati aziendali quando si ha a che fare con operazioni straordinarie, partnership e quindi situazioni in cui si condividono con un altro soggetto informazioni rilevanti per l'azienda?

In relazione alla gestione della partnership il GDPR prevede che si instauri una "privacy chain", ovvero un sistema che permetta al Titolare di nominare organizzazioni Responsabili che presentino garanzie adeguate e di controllare che le nomine dei sub-responsabili, da questi effettuate, assicurino opportuni requisiti. Il DPO, in tale frangente esercitando un audit di seconda parte consente di assicurare le garanzie della privacy chain.

L'efficacia della privacy chain troverà un utile strumento nella ISO 27552 (Enhancement to ISO/IEC 27001 for privacy management), che verrà pubblicata a metà del 2019. Nel frattempo è necessario predisporre specifiche clausole contrattuali vincolanti per le organizzazioni responsabili e sub-responsabili.

>>> SEGUE DALLA PRIMA PAGINA

GDPR, DA OBBLIGO GIURIDICO AD ASSET COMPETITIVO

MEO (PORTAVOCE GARANTE PRIVACY): "AZIENDE ATTENTE A PREPARARSI PER LE NUOVE NORME. È NECESSARIO UN APPROCCIO SISTEMICO"

> CAMBIA IL RUOLO DEL GARANTE, CHE AVRÀ FUNZIONE DI CONTROLLO A POSTERIORI RISPETTO ALLE SCELTE SUL TRATTAMENTO CHE SPETTANO AI TITOLARI

Sullo stato di adeguamento delle aziende italiane alla normativa il giudizio a oggi è sufficiente o no?
Il mondo imprenditoriale è consapevole dell'impatto che il Regolamento Ue avrà sull'organizzazione e sulle procedure da mettere in atto e sta dimostrando di essere attento a non farsi trovare impreparato alla scadenza del 25 maggio; ciò vale soprattutto per quelle imprese che hanno operato bene negli ultimi 20 anni, da quando cioè in Italia è in vigore una normativa specifica sulla protezione dei dati, rispetto alla quale il Regolamento non rappresenta in realtà una rivoluzione, ma una evoluzione. Il Regolamento non dovrebbe essere tuttavia essere visto come un aggravio, ma come un'opportunità per sottoporre ad una revisione complessiva tutti i processi e le modalità di la gestione dei dati alla luce dei nuovi contesti tecnologici e dei nuovi bisogni di tutela espressi dalle persone. La protezione dei dati personali deve rappresentare per le imprese non tanto e non solo un obbligo giuridico quanto, piuttosto, una componente strategica, un asset competitivo e una competenza da sviluppare all'interno dell'organizzazione aziendale. Per quanto l'apparato sanzionatorio introdotto dal Regolamento sia particolarmente robusto, non può essere l'unico aspetto in grado di assorbire tutte le preoccupazioni delle imprese.
La nuova normativa impone nuovi livelli di professionalità e di organizzazione e pone un accento diverso sulla sicurezza dei sistemi, anche in caso di esternalizzazione.
La sicurezza del patrimonio informativo dell'impresa e dei sistemi che conservano i dati non costituisce più un elemento accessorio e strumentale, ma richiede un approccio sistematico. La sicurezza dei dati è già oggi, ed è destinata a diventarlo sempre di più, il presupposto essenziale per la liceità dei trattamenti e per assicurare che i dati siano sempre integri, corretti e aggiornati.
Diversi sono gli istituti presenti nel Regolamento volti alla prevenzione del rischio, tra i quali anzitutto la già ricordata valutazione d'impatto Funzione preventiva hanno anche le misure di protezione adottate fin dalla progettazione (*privacy by design*) o per impostazione predefinita (*privacy by default*), finalizzate ad assicurare delle garanzie indispensabili per la tutela dei diritti degli interessati e la minimizzazione del rischio connesso alle operazioni svolte.
Analoga funzione ha anche l'obbligo di notifica dei *data breach* da cui possano derivare rischi per i diritti e le libertà degli interessati, da svolgersi entro 72 ore e comunque senza ingiustificato ritardo.
I responsabili del trattamento, cioè le aziende e gli enti che trattano dati in outsourcing, sono tenute a collaborare con i titolari nella definizione delle misure tecniche e organizzative adeguate e devono inoltre rispettare una serie di obblighi che li riguardano direttamente e che sono ispirati agli stessi principi di *accountability* che valgono per i titolari.
In cosa cambia il rapporto Garante-azienda con il Gdpr?
Il Regolamento come detto ha un approccio basato sulla prevenzione rischio e sulla responsabilizzazione dei titolari del trattamento, che devono mettere in atto comportamenti proattivi ed essere grado di dimostrare di aver concretamente adottato misure finalizzate ad applicare la nuova disciplina e a proteggere i dati. L'intervento dell'Autorità sarà di accompagnamento dell'implementazione delle norme, da un lato, e sempre più di verifica e accertamento del rispetto di tali norme. Dall'altro sarà un controllo svolto principalmente "a posteriori", che si collocherà in una fase successiva a quella delle scelte assunte dal titolare. Così si spiegano anche alcune riduzioni di oneri, come l'abolizione dell'obbligo di notificare i trattamenti al Garante e di chiedere una "verifica preliminare" (*prior checking*), e l'introduzione, per altro verso, di un obbligo di consultazione del Garante all'esito della valutazione di impatto svolta dal titolare che segnali il permanere di un rischio residuale elevato per i diritti degli interessati. In questa prospettiva, il Regolamento punta anche a semplificare il quadro giuridico e a razionalizzare gli oneri amministrativi, che la Commissione Ue stima in 130 milioni di euro di risparmi annui per le aziende europee. ■

>>> DALLA PRIMA PAGINA

SANZIONI E DANNI DI IMMAGINE: RISCHI PER LE IMPRESE NON PROTETTE

ANDREA BORGHI (SICUREZZA SISTEMI MULTIPARTNER): "QUESTI FATTORI LEGATI AL TRATTAMENTO DATI SI TRADUCONO RAPIDAMENTE IN PERDITA DI QUOTE DI MERCATO"

Questi rischi, che possono poi tradursi in danni in primo luogo reputazionali, - spiega la responsabile Sicurezza Sistemi di Multipartner - impongono "una adeguata formazione" che aiuti a sviluppare "una sensibilità aziendale nuova" rispetto a queste tematiche.

Protezione dei dati sensibili e privacy: quali sono i rischi in cui un'azienda può incorrere adottando comportamenti sbagliati?

Il mondo di oggi gira e si regge sull'informazione, e quella personale e sensibile ha un valore elevato che va tutelato e protetto. Sostanzialmente i principali fattori di rischio per un'azienda che non protegge adeguatamente i suoi dati adottando i comportamenti, le misure e le metodologie necessarie, sono diversi. C'è un rischio diretto dell'azienda che, non rispettando le policy di tutela e trattamento dati così come previste dal GDPR, può incorrere in pesanti sanzioni; ci sono danni all'immagine e alla reputazione aziendale che si traducono quasi istantaneamente in danni economici e perdita di quote di mercato; se in azienda poi, non si trattano adeguatamente dati appartenenti a "terzi", i rischi a cui ci si espone derivano da eventuali controversie legali ad opera proprio delle terze parti. Di queste "nuove" responsabilità le aziende ora devono farsi necessariamente carico.

Gli errori umani costituiscono spesso una fonte di rischio importante di perdita di controllo sull'integrità dei dati?

Proteggere e tutelare i dati, per quanto costoso, è fattibile. Il principale punto debole rimane sempre l'interazione con e tra le persone, le quali possono essere una fonte di rischio per incuria, per ignoranza intesa come non conoscenza o peggio, per dolo. Per queste tre ragioni, di fatto, può accadere che l'accesso - pur ufficialmente verificato e autorizzato - di una persona alla consultazione o alla gestione di dati e documenti cosiddetti sensibili, possa generare seri problemi che mettono a rischio l'integrità stessa del dato, oltre che l'azienda nel suo complesso. È quindi estremamente importante creare nelle aziende la cultura della sicurezza attraverso un'adeguata formazione. Va sviluppata una sensibilità aziendale nuova rispetto alle tematiche di tutela e protezione dei dati che sia trasversale, a partire dai vertici fino ad arrivare alle figure che quotidianamente se ne occupano. La sensibilizzazione e la formazione rispetto alla nuova normativa GDPR e le maggiori responsabilità che ne derivano possono risultare decisive nell'acquisire chiara consapevolezza di eventuali comportamenti sbagliati adottati in passato e agire da barriera frangiflutto, impedendo automaticamente un flusso di azioni errate e dannose.

"IL PRINCIPALE PUNTO DEBOLE È L'ERRORE UMANO, CHE PUÒ METTERE A RISCHIO L'INTEGRITÀ DEI DATI. SERVONO FORMAZIONE E SENSIBILITÀ AZIENDALE VERSO LE TEMATICHE DI TUTELA E PROTEZIONE

Come si stanno attrezzando, soprattutto dal punto di vista tecnologico, in vista dell'entrata in vigore della nuova normativa GDPR?

Le aziende si stanno attrezzando iniziando principalmente a fare assessment interni sulle proprie posizioni rispetto a sicurezza, tutela e protezione dei dati. Gli assessment permettono di individuare rapidamente le proprie mancanze e di ottenere, se necessario, le "prime indicazioni" delle misure tecniche ed organizzative da adottare per raggiungere la conformità al Regolamento Generale sulla Protezione dei Dati UE. Ciò comporta a volte, la necessità di ridisegnare la geografia dei propri processi aziendali e la conseguente attivazione di tutte quelle misure correttive necessarie sia in termini di tecnologia, sia in termini di risorse umane. Ma il risultato principale sembra essere quello che le aziende, così facendo, stiano iniziando a sviluppare attenzione e consapevolezza rispetto ai rischi legati al "non essere compliant". Allo stesso tempo la conoscenza della normativa permette di trovare la giusta collocazione rispetto a quanto richiesto dal GDPR senza necessariamente scoprire di dover riorganizzare tutti i propri processi interni ma magari effettuando correzioni sulle procedure interne di gestione, solo se ne sussistono le condizioni.

SECURITY: POCHI GRUPPI CON STRUTTURA CHIARA

Le aziende italiane vanno a passo lento nel creare una struttura interna di gestione della security: circa la metà delle grandi imprese si è dotata della figura del Chief Information Security Officer; nel 18% delle imprese è presente un Data Protection Officer. Questo è quanto emerge dall'ultima indagine dell'Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano relativa al 2016. Secondo lo studio le aziende hanno investito 972 milioni complessivi in soluzioni di Information Security ma solo il 39% ha un piano pluriennale di interventi.

I progetti più diffusi riguardano principalmente l'identificazione dei rischi e la protezione dagli attacchi, meno attenzione sulla rilevazione degli eventi, risposta e ripristino. I principali rischi per gli ambienti cloud arrivano dai rapporti con i fornitori e derivano per lo più dalla mancanza di controllo sulle operations del service provider. Anche le pmi dedicano un budget all'information security al fine di adeguarsi alle norme e in risposta ad attacchi subiti.