Molte imprese in ritardo nell'individuazione dei soggetti che si devono occupare di privacy

Data protection officer, audit per poter partire a maggio '18

Pagine a cura di **Federico Unnia**

Il conto alla rovescia prosegue inesorabile. Mancano meno di nove mesi all'entrata in vigore del regolamento comunitario sulla protezione dei dati personali (25 maggio 2018). Le imprese e gli studi legali specializzati si stanno affrettando a mettere ordine nelle procedure interne e trovare quelle competenze necessarie a formare professionisti in grado di gestire e dialogare con il Garante per la privacy, cioè i Dpo, acronimo di *Data Protection Officers*. Secondo **Bridget Ellison** dello Studio ***De Berti Jacchia Franchini Forlan,*** «la difficoltà maggiore è di acquisire una nuova cultura della privacy in quanto finora era spesso considerata una semplice questione di forma e un costo senza benefici. Ora dovrà essere incorporata come parte integrante nei processi aziendali stessi, in ogni attività nell'ambito della quale vengono trattati i dati personali».

Bridget Ellison

Le imprese hanno il problema di identificare correttamente quali dei nuovi obblighi imposti dal regolamento siano applicabili nel loro caso specifico, di come organizzarsi per far fronte ai nuovi diritti degli interessati, e della gestione della sicurezza dei dati in presenza di una maggiore flessibilità in questo riguardo, ma anche della necessità di essere in grado di poter dimostrare la conformità alle norme.

«Occorre mettere in atto un piano, con l'assistenza di consulenti in materia giuridica, gestionale e tecnica, che preveda un'analisi della situazione esistente per arrivare ad un'analisi di rischio e del gap tra la situazione riscontrata e una piena conformità alle nuove norme. In base ai risultati di tali analisi, si procede a definire un modello di gestione della privacy (*privacy by design*).

È essenziale una grande attenzione alla formazione di tutte le persone coinvolti nel trattamento dei dati personali in ogni contesto aziendale» chiosa la Ellison.

Cristina Martorana

Secondo **Cristina Martorana**, partner di ***Orrick*** (opera nel team Privacy/Data Protection composto anche da **Alessandro De Nicola** e **Marco Dell'Antonia**), «dipende dalla sensibilità che l'impresa stessa ha dimostrato in passato verso la compliance. Nella nostra esperienza, per le imprese - soprattutto se di respiro extraterritoriale - che hanno da sempre avuto una naturale propensione a farsi parte attiva verso la compliance, il nuovo Regolamento rappresenta un'opportunità, dato che porterà una maggiore uniformità normativa non solo all'interno dell'Unione ma anche rispetto a soggetti imprenditoriali che pur non avendo sede nell'Unione trattano dati di controparti, clienti o altro residenti nell'Unione. Inoltre una maggiore responsabilizzazione dei titolari del trattamento».

Lorenzo Conti

«Per le imprese che hanno fino ad oggi sostanzialmente sottovalutato la privacy, pensando fosse un adeguamento «burocratico» ma non sostanziale», aggiunge Martorana, «il nuovo Regolamento rappresenta una grossa sfida, che si vince solo con un profondo cambiamento culturale. Il nuovo sistema sanzionatorio potenzialmente applicabile aiuterà il processo di sensibilizzazione. Saranno cruciali due competenze: quella legale, con un focus sulla compliance, e quella tecnico informatica».

Come affrontare i mesi che mancano al 25 maggio 2017? «Conviene affrettarsi» chiosa **Lorenzo Conti**, partner dello ***Studio Legale Rucellai & Raffaelli*** e responsabile del team di Data privacy. «Le aziende più virtuose si stanno già attrezzando da tempo. In particolare andranno ridefiniti i modelli di gestione della privacy in azienda, scegliendo tra il criterio della Privacy by design e quello della Privacy by default a seconda delle diverse realtà aziendali. Viene inoltre introdotto l'obbligo di tenuta del Registro dei Trattamenti. Come studio procediamo insieme al cliente con un preliminare data *privacy assessment* e conseguentemente alla definizione dei gap sui quali intervenire insieme, dando priorità ai processi che implicano il trattamento dei dati più delicati, per poi procedere alla predisposizione di un nuovo modello privacy che sia conforme al nuovo Regolamento e alla relativa formazione in azienda».

Giangiacomo Olivi

Giulio Coraggio

«Per soddisfare i requisiti e gli adempimenti richiesti dal nuovo regolamento, è necessario effettuare una mappatura di tutti i trattamenti: in estrema sintesi, conoscere e poter dimostrare di sapere, quali dati personali vengono raccolti, per quali finalità, per quanto tempo vengono conservati, per quale motivo vengono raccolti, a chi viene dato accesso e perché, come vengono protetti, a chi vengono comunicati e perché» spiega **Giangiacomo Olivi**, partner, responsabile del dipartimento Ipt di ***Dla Piper*** in Italia. «Una mappatura precisa e aggiornata è il punto di partenza. Non si tratta quindi solo di mettere mano a documenti, ma di pensare, o ripensare, a come e perché si trattano determinate informazioni. Tutto ciò andrà accompagnato da una adeguata e costante opera di educazione aziendale alla protezione dei dati personali».

«Nell'assistere vari clienti abbiamo identificato 4 problematiche che si ripetono frequentemente«, dice a *Affari Legali* **Giulio Coraggio**, partner del dipartimento IP&T e responsabile del settore technology di ***Dla Piper*** Italia: «esiste un accesso diffuso e spesso ingiustificato ai dati dei clienti da parte non solo dei dipendenti delle società, ma a volte anche i loro agenti. Ciò è di solito la conseguenza di un approccio «pigro» alla definizione dei profili di accesso perché è più facile concedere un accesso a tutti che dover fare una selezione delle applicazioni da abilitare. Manca poi un inventario dei trattamenti e quindi di quali dati sono trattati, da chi, per quali finalità, dove sono conservati e a chi sono comunicati. Questo è dovuto anche alla mancanza di sistemi di data management che sono fondamentali al fine di poter tracciare i dati e gestirli correttamente in caso, ad esempio, di esercizio del diritto alla portabilità, qualora si verifichi un data breach, o nel caso in cui i dati debbano essere cancellati o anonimizzati per la scadenza del termine di conservazione. In terzo luogo viene eseguito un trattamento non del tutto conforme al consenso ottenuto dai relativi individui. Ciò accade spesso per esempio con la profilazione dei clienti che ormai è eseguita da quasi tutte le società, ma senza che sia ottenuto un consenso separato relativo specificatamente a tale finalità. Infine, mancano dei controlli tecnici e organizzativi sul trattamento dei dati, sia con riferimento ai sistemi informatici delle società, sia ai fornitori o agenti che trattano i dati per conto della stessa. Spesso tali controlli sono puramente formali e non vi corrispondono delle verifiche effettive sul corretto trattamento».

Gianluca de Cristofaro

Dal canto suo **Gianluca de Cristofaro**, partner di ***LCA Studio Legale*** sottolinea come «l'introduzione del principio di accountability ha dei riflessi considerevoli sull'organizzazione aziendale. La società che effettua trattamenti di dati personali deve studiare e attuare procedure interne le cui finalità sono quelle di rendere effettiva la compliance dei processi ai principi e obblighi previsti dal Regolamento e mantenere evidenza e dimostrare – con onere a proprio carico – il rispetto dei principi e obblighi previsti dal Regolamento. Occorre quindi muoversi in fretta».

Secondo **Flaviano Sanzari,** dello ***Studio Previti,*** «il nuovo Regolamento Eu 679/2016 cambia innanzi tutto l'approccio al «problema» privacy, introducendo i principi della privacy by default e by design. Per le aziende l'impatto è significativo e coinvolge varie funzioni, a partire dall'organizzazione. Le imprese e le pubbliche amministrazioni per le quali sarà obbligatorio istituire il Dpo, ad esempio, dovranno dotarsi di questo nuovo ufficio; saranno poi coinvolti gli uffici legali e tecnici, essen-

Supplemento a cura di **Roberto Miliacca** ***rmiliacca@class.it*** *e* **Gianni Macheda** ***gmacheda@class.it***

Gli obblighi imposti dal regolamento Ue vanno spiegati

Flaviano Sanzari

do necessario istituire nuovi processi interni e dotarsi di nuovi strumenti tecnologici, nella maggior parte dei casi. Dipende poi, ovviamente, dallo stato di fatto dal quale si parte. Per le aziende già in regola con l'attuale Codice Privacy le difficoltà saranno ovviamente minori. Quello che non si deve fare è sottovalutare l'impegno necessario per arrivare pronti alla scadenza del 25 maggio 2018, anche in considerazione del regime sanzionatorio che il nuovo Regolamento introduce. Per le violazioni più importanti – come quelle che riguardano, ad esempio, i principi base del trattamento, il consenso dell'interessato, i diritti degli interessati – sono previste sanzioni fino al 4% del fatturato mondiale annuo dell'impresa o sino a 20 milioni di euro».

Massimiliano Masnada

Massimiliano Masnada, counsel, responsabile del team di privacy e data protection di ***Hogan Lovells*** in Italia, punta l'attenzione sulle difficoltà principali per sono relative ai nuovi obblighi che impone il Regolamento con particolare riferimento al principio della cd. accountability, ossia l'obbligo di adozione di approcci e politiche aziendali che tengano conto costantemente del rischio per la privacy degli interessati.

«Questo principio si manifesta nell'obbligo di privacy-by-design volto a garantire che gli strumenti e i sistemi di trattamento di dati personali utilizzati sin dall'inizio siano pensati per rispettare la privacy nonché nell'obbligo di effettuare una valutazione di impatto di tutte le attività di trattamento che comportino un elevato rischio per la libertà e i diritti delle persone fisiche. Poi vi è l'obbligo di nomina del Responsabile della protezione dei dati (Dpo) per le imprese che trattino su larga scala categorie particolari di dati (es dati sensibili e giudiziari) ovvero che facciano un'attività di monitoraggio regolare e sistematico su larga scale degli interessati (es. provider di internet). Tale nuova figura, che riferisce solo ai vertici aziendali, avrà compiti consultivi e di sorveglianza e sarà l'interfaccia della Autorità di controllo. Un'altra novità importante saranno i diritti alla «portabilità» dei dati personali e alla limitazione del trattamento» aggiunge.

Dal canto suo, Hogan Lovells ha appena lanciato una app innovativa e gratuita, per Ios e Android, chiamata *GDPRNow*. È la prima creata internamente e interamente in uno studio legale ed elaborata dal team di data protection e cyber security. Ogni società che la scarica, dopo una prima check list, spiegano dallo studio, potrà generare il proprio action plan e scaricare un report su misura con le azioni da porre in essere da qui a un anno per essere pienamente compliant con il regolamento. La app è utile per le aziende in ogni settore industriale e permette di stilare un action plan con le varie priorità.

Secondo **Simona Lavagnini** di ***LGV Avvocati,*** «occorrerà mantenersi sempre aggiornati su chiarimenti o Linee Guida forniti dalle autorità europee e nazionali. Tale attività riguarderà l'aggiornamento della documentazione in uso (anche alla luce dei nuovi diritti dell'interessato introdotti dal Regolamento, come il diritto alla portabilità), l'adozione delle procedure volte a consentire l'esercizio dei diritti degli interessati, la formazione dello staff, la revisione e l'implementazione di misure tecniche e organizzative adeguate, la nomina di un Privacy Officer, l'implementazione di procedure per la comunicazione delle violazioni dei dati personali («data breach») e l'adozione di un registro delle attività di trattamento e di procedure per il suo aggiornamento».

Parla di forte discontinuità rispetto al passato, **Nadia Martini,** head of Data Protection (Italy) Certified Privacy Officer IP & IT Expert, partner associate di ***Rödl & Partner***, secondo la quale «Il cambiamento più significativo è il rivoluzionario cambio culturale: si passa da una privacy percepita formale, dove bastava fare il minimo previsto dalla legge, a una privacy sostanziale dove occorre fare quanto le imprese valutano e dimostrano essere la soluzione più adeguata al loro caso concreto, tenendo conto dei trattamenti posti in essere e del relativo livello di rischio. La nuova disciplina impatta in modo trasversale i diversi business, ovvero tutti i settori che trattano dati personali di persone fisiche: quelli più interessati sono il mondo IT, Farmaceutico, Media, Sanitario, Web, e-commerce, IoT, Fashion, Food, Recupero Crediti, la Pa e tanti altri ancora. In tutti questi casi, vengono trattati grandi volumi di dati personali, si pensi alla profilazione

Nadia Martini

tipica del modo e-commerce o al telemonitoraggio nel modo sanitario. Ma anche il settore B2B, tipico delle imprese industriali non è escluso».

Per **Giuseppe Vaciago,** partner di ***R&P Legal*** e docente di informatica giuridica all'Università dell'Insubria, «è necessario comprendere il proprio livello di compliance dell'attuale normativa nazionale prevista dal dlgs. 196/03. Molte società non

Giuseppe Vaciago

hanno ancora una corretta consapevolezza del provvedimento del Garante sugli amministratori di sistema (provvedimenti del garante del 27 novembre 2008 e del 26 giugno 2009) esattamente come hanno deciso di abbandonare la tenuta del Dps (Documento programmatico sulla sicurezza) dopo che ne è stata dichiarata nel 2012 la non obbligatorietà. Dopo aver fatto questa analisi è necessario iniziare ad analizzare i temi più propri del Regolamento con la cautela di chi deve affrontare una materia nuova che potrebbe essere soggetta a numerose interpretazioni in corso d'opera in grado di modificare il tipo di approccio tenuto fino a quel momento. Il Garante per la protezione dei dati personali ha già emanato delle prime linee guida in materia ma speriamo che nel prossimo futuro vi siano ulteriori documenti chiarificatori».

Infine, punta l'attenzione sulle imprese di più piccole dimensioni **Silvia Stefanelli**, co-fondatrice di ***Stefanelli&Stefanelli Studio legale***, secondo la quale «il nuovo regolamento ha un amplissimo ambito di applicazione. Senza dubbio, sotto il profilo soggettivo, le piccole imprese sono quelle che probabilmente faranno più fatica a gestire il dato secondo i principi del risk management; sotto il profilo oggettivo poi saranno i titolare di dati sensibili e su larga scala ad essere chiamati a maggiori adempimenti. Credo però che la nuova disciplina vada colta anche nelle sua sfide positive: il dato è considerato oggi «the new gold» per la sua enorme potenzialità di marketing ed allargamento del mercato, ma anche in quanto strumento di controllo, monitoraggio e gestione aziendale. Perché quindi non sfruttare questo obbligo legislativo per potenziare i proprio management aziendale? «.

Silvia Stefanelli

© Riproduzione riservata

VINCENZO COLAROCCO, *PREVITI*

La Lombardia punta sulla videosorveglianza

Prudenza sulla videosorveglianza dei lavoratori in azienda: vanno sempre tenute in considerazione le regole in materia di protezione dei dati personali. La Regione Lombardia, con la legge n. 2 del 22 febbraio 2017, attraverso l'erogazione di contributi, sta favorendo l'installazione di sistemi di videosorveglianza a circuito chiuso nelle residenze sanitarie assistenziali (Rsa) e nelle strutture residenziali e semiresidenziali per disabili (Rsd) pubbliche e private accreditate. Ciò al fine di migliorare il livello di sicurezza dei servizi erogati nelle Rsa. La Regione ha messo a disposizione fondi sino a 1,4 milioni di euro per finanziare almeno il 50% delle spese sostenute per l'installazione dei sistemi di videosorveglianza di cui sopra. «Le criticità e le responsabilità derivanti dall'installazione dei sistemi di videosorveglianza derivano dall'applicazione della normativa sulla protezione dei dati personali» spiega **Vincenzo Colarocco** dello ***Studio legale Previti***. «In particolare dovrà tenersi conto sia delle tipologie di videocamere che verranno adottate, sia dei luoghi dove verranno installate, in quanto vi è il rischio che possano essere utilizzate per effettuare controlli sui lavoratori. Pertanto, al fine di evitare sanzioni amministrative e responsabilità civili e penali, gli impianti di videosorveglianza dovranno essere installati nel rispetto delle normative in materia di tutela dei lavoratori e protezione dei dati personali.

Vincenzo Colarocco

Domanda. La nuova disciplina della Lombardia potrebbe essere estesa anche a livello nazionale?

Risposta. Sarebbe auspicabile che la legge regionale in esame venga estesa a livello nazionale, in quanto gli incentivi volti all'implementazione di misure di sicurezza efficienti, che fungono anche da deterrente per la commissione di illeciti, migliorano la sicurezza in ambienti nei quali spesso, come si è potuto apprendere da numerosi episodi di cronaca, tale sicurezza non viene garantita, soprattutto agli ospiti di dette strutture. Sotto gli altri profili, l'eventuale estensione a livello nazionale porrebbe le stesse questioni di cui si è già accennato, per cui andrebbero regolate bene le interferenze con la tutela dei diritti dei lavoratori e con la tutela dei dati personali in genere.