GDPR, iniziate le verifiche sul campo. Le proposte del Laboratorio per la Sicurezza per la compliance delle aziende del Retail

a cura della Redazione

Com'era nelle previsioni, il Garante per la privacy ha dato inizio alle ispezioni sul rispetto del **Dlgs 101/2018** (che recepisce il GDPR per l'Italia) avvalendosi della Guardia di Finanza. In base alla programmazione semestrale, i primi controlli hanno riguardato tre settori: finanza, sanità e le carte fedeltà, queste ultime tipicamente utilizzate da GDO e retailer.

Proprio dall'esperienza della verifica ricevuta nel mese di maggio da un retailer con propri security manager aderenti al Laboratorio per la Sicurezza, l'associazione ha ritenuto di sviluppare un *case study* per indicare alle altre aziende i comportamenti più corretti al fine di non incorrere nelle sanzioni previste dal GDPR **(leggi)**.

Il caso verrà presentato il 2 ottobre prossimo nel corso di un seminario organizzato al FICO di Bologna dal Laboratorio assieme a MYDPO.

Nell'intervista che segue, **Bruno Frati** e **Fabio Guarino**, rispettivamente DPO e security manager dell'azienda controllata, sintetizzano le indicazioni per risultare adempienti in caso di ispezione.

Giuseppe Mastromattei, presidente del Laboratorio per la Sicurezza, delinea infine un programma per formare e sostenere i security manager aderenti all'associazione sui temi specifici della compliance al GDPR.

Bruno Frati, DPO

In che modo un retailer operante a livello nazionale deve predisporsi per dimostrare la propria volontà di essere compliant al GDPR in caso di verifica richiesta dal Garante?

In caso di ispezione in ambito privacy, l'azienda dovrà dimostrare - fin dalla prima fase della verifica – di non aver adempiuto soltanto a livello formale, ma di aver intrapreso un percorso di sensibilizzazione capillare rivolto a tutti i livelli/aree aziendali. In tal modo sarà possibile individuare immediatamente la figura di riferimento in caso di verifica. Si ritiene che la rapidità e la prontezza in questo primo passaggio possano, almeno in parte, determinare l'andamento delle fasi successive.

Ovviamente è fermamente consigliabile un atteggiamento collaborativo e proattivo da parte del Titolare. Risulta altresì opportuno concentrarsi sulle richieste/quesiti formulati dall'organo ispettivo, fornendo la documentazione inerente e le valutazioni che giustificano le scelte effettuate in materia. In altre parole, è necessario arginare il rischio di andare fuori tema. Centrale diventa quindi la figura del Data Protection Officer che coordinerà e guiderà le figure aziendali coinvolte.

Quale assistenza deve dare il DPO in caso di verifica della GdF in azienda?
Il DPO, quale attore principale, è tenuto a dare piena disponibilità durante le giornate di ispezione che solitamente hanno una durata di tre giorni lavorativi.
Dovrà infatti recarsi al più presto presso la sede della società e assistere il Titolare o suo delegato fino alla fase finale e, anche successivamente, al fine di produrre ulteriore documentazione nei termini indicati dall'Autorità Garante.
Oltre alla documentazione attestante l'attività svolta periodicamente dal DPO (come verbali di incontri, valutazioni, etc.), lo stesso dovrà dare prova del suo coinvolgimento in azienda e di conoscere in modo approfondito le dinamiche proprie della realtà di riferimento.

Fabio Guarino, security manager

Quali sono state le modalità delle prime verifiche condotte dalla GdF su indicazione del Garante e quali sono stati i punti di maggior attenzione da parte degli ispettori?
Nel caso della nostra azienda, la visita era orientata sul controllo di tutto ciò che fosse legato al "programma fedeltà" dei clienti e alla gran mole di dati personali che vengono raccolti ogni giorno nei nostri negozi o attraverso il sito internet. E' stato un controllo molto dettagliato per individuare dapprima chi sono i soggetti coinvolti in tale tipo di trattamento, verificando le corrette nomine degli stessi, e poi, in maniera più approfondita, per comprendere in che modo questi dati vengono raccolti, archiviati e utilizzati. Non è mancato un approfondimento sulla struttura della rete aziendale e sulla dislocazione dei server e sulla gestione della loro sicurezza.
Durante l'intera ispezione sono state due le parole chiave:
La prima è stata sicuramente **accountability** ovvero dar conto di ogni decisione presa e dimostrare di aver agito con responsabilità seguendo linee guida coerenti e adatte al tipo di trattamenti svolti, e che le misure adottate fossero state scelte perché adeguate.
La seconda parola è stata **documentazione**; durante tutto il periodo dell'ispezione, i militari del nucleo speciale privacy, hanno raccolto ogni tipo di documento che potesse dimostrare le azioni fatte: documenti che attestassero la formazione svolta; e-mail di convocazione di riunioni; circolari inviate al personale e tutto quello che era ritenuto utile a dimostrare le dichiarazioni rilasciate.
La presenza del DPO è stata richiesta da subito ed è stata sicuramente fondamentale; la nostra azienda ha, negli anni, emesso diverse migliaia di carte fedeltà e la quantità raccolta di dati personali, in particolare anagrafici, non è da poco. Aver avuto a disposizione il DPO e i consulenti che ci hanno seguito durante la fase di adeguamento al GDPR, è stato di grande aiuto per spiegare e sostenere le decisioni prese nell'amministrazione dei dati e nella gestione degli accordi con tutte le figure che hanno accesso agli stessi, come eventuali contitolari del trattamento e responsabili esterni.

Quali indicazioni si possono trarre per le aziende del retail da queste prime esperienze dirette?
La prima cosa da fare è sensibilizzare la direzione aziendale. Frasi come *"tanto è la privacy"* o *"basta sistemare le carte"* devono sparire dalla mentalità e dalla struttura di governance. Le sanzioni elevate e la responsabilità del Titolare del trattamento dei dati sono sicuramente un buon approccio per far comprendere quanto burocrazia e standardizzazione siano inadatte alla realizzazione dello scopo.
Fondamentale è stato avere un gruppo di lavoro all'interno dell'azienda che si occupasse della materia, soprattutto per informare i colleghi e per tracciare la grande quantità di trattamenti effettuati. Incontri periodici di formazione e la sensibilizzazione delle varie funzioni aziendale, hanno permesso di non lasciare fuori alcun trattamento e di non trovarsi in situazioni spiacevoli durante l'ispezione. Il nostro gruppo è costituito da un Manager dell'HR, dal Responsabile IT e dal Responsabile Security e Loss Prevention; questo è l'unico modo per avere una visione di insieme di quelli che sono i problemi e per approcciare al meglio alle soluzioni.

Qualcuno mi ha chiesto come mai la funzione Security e Loss Prevention fosse coinvolta nella gestione di questi processi. Le risposte sono sostanzialmente due:

- *i dati fanno parte del patrimonio aziendale, in particolare nelle aziende del retail. Chi se non la funzione che si occupa della difesa del patrimonio può occuparsene?*
- *il security manager ha una visione della valutazione dei rischi che altre funzioni, in generale, non hanno. Per dimostrare di aver adottato misure adeguate, bisogna aver valutato in maniera più completa possibile tutti i possibili rischi.*

Giuseppe Mastromattei, presidente Laboratorio per la Sicurezza

Il Regolamento Generale sulla Protezione dei Dati (Regolamento UE 679/2016, noto anche come GDPR) ha introdotto, con l'articolo 25 l'obbligatorietà per tutte le organizzazioni di applicare il principio di protezione dei dati fin dalla progettazione. Un principio, sintetizzato come *privacy by design*, assolutamente innovativo per le aziende italiane.

Il concetto di *"privacy by design"* si riferisce soprattutto alle misure di sicurezza, ma quali utilizzare, quali considerare? Anche alla luce del fatto che il mondo del Retail è in continua innovazione e, soprattutto, un settore che sempre di più cerca di creare esperienze di shopping personalizzate attraverso offerte, attività promozionali e comunicazioni che avvengono su piattaforme omnicanale?

Un approccio alla protezione dei dati personali non più statico, ma che evolve con il tempo, dinamico, proprio come lo è il mondo del Retail.

Ecco quindi la necessità di confrontarsi costantemente, condividendo ogni esperienza e ogni nuova misura di sicurezza, ma anche condividendo quelli che possono essere i risultati di una attività ispettiva effettuata presso una delle aziende rappresentate nel "Laboratorio".

La protezione del dato personale oggi è una priorità globale, in un mondo in continua evoluzione, uscire dai propri confini è determinante, soprattutto per le aziende.

Proprio per questo motivo l'evento organizzato dall'Associazione "Laboratorio per la Sicurezza", previsto il prossimo 2 ottobre a Bologna, sarà una importante occasione per discutere ed analizzare congiuntamente, come proteggere al meglio i dati dei clienti del mondo del Retail, e quale progettazione di un sistema di sicurezza possa risultare, in questo specifico momento, più idonea.

In particolare, con riferimento al primo comma dell'articolo 25 del GDPR che testualmente dice: *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati".*

Potremmo sintetizzare gli argomenti dell'incontro secondo i seguenti punti:

- *Quale è lo stato dell'arte, con particolare riferimento al mondo del Retail ed ai suoi clienti;*
- *I costi di attuazione e come garantire misure tecniche ed organizzative adeguate;*
- *Come soddisfare i principi, sanciti nel GDPR per garantire una efficace protezione dei dati.*

Alla fine, anche la condivisione, è uno dei principi alla base del concetto di *"privacy by design"*, ed è proprio il Laboratorio il posto ideale dove creare **#Contaminazione**, ovviamente in senso positivo.