FISCALFOCUS.it

4 giugno 2018

PRIVACY. LE ISPEZIONI E I CONTROLLI DELLA GUARDIA DI FINANZA

LE SANZIONI APPLICATE DAL GARANTE DELLA PRIVACY

A pochi giorni dall'entrata in vigore del nuovo Regolamento (Ue) sulla privacy, le domande più frequenti nei vari settori sono tutte incentrate sulle, possibili, nuove attività ispettive e di controllo generate dal nuovo sistema.

La riforma sulla privacy introduce **importanti novità** anche riguardo alle **modalità ispettive**. Se prima, infatti, i controlli si basavano su una serie di domande e una lista di controlli ai quali, in caso di violazioni, seguivano sanzioni dai 150 ai 300.000 euro, ora invece in sede ispettiva avrà fondamentale importanza il concetto di **accountability** (responsabilizzazione). In caso di controlli sarà di fondamentale importanza dimostrare di aver adottato **in maniera preventiva** tutte le misure di protezione necessarie (ciò che appunto il principio dell'accountability richiede), compresa l'analisi del rischio in fase iniziale/progettuale.

Secondo tale principio, infatti, il titolare del trattamento deve aver messo in atto **adeguate misure tecniche ed organizzative per garantire ed essere in grado di dimostrare** che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina. Altra caratteristiche di tale principio è che spetta al titolare del trattamento dei dati scegliere quali sono gli strumenti adatti per implementare il regolamento.

Se, dunque, il titolare del trattamento potrà dimostrare di essersi conformato al principio - che è alla base di tutto il Regolamento - secondo cui i problemi e le soluzioni da adottare devono essere valutati a monte nella fase di progettazione come impostazione predefinita (privacy by default) ovvero secondo il principio del "prevenire anziché correggere", non avrà nulla da temere.

Ma se ciò non dovesse verificarsi, come il caso di molte aziende o uffici professionali che non sono riuscite ad adeguarsi in tempo utile, a cosa si va incontro?

Ebbene, va innanzitutto precisato che il vecchio Codice della privacy e le sue regole (la "check

list" che veniva utilizzata in fase di controllo e le sanzioni che a esso si riferivano) sono totalmente superate con l'arrivo del nuovo Regolamento.

Si aggiunga che nulla conta il fatto che nel nostro Paese non ci sia ancora il Decreto di adeguamento e che ci sia la proroga alla delega al 21 agosto 2018 dal momento che le sanzioni sono, comunque, pienamente applicabili dal giorno stesso in cui il Regolamento ha fatto la sua entrata ufficiale, ossia il 25 maggio.

Ma andiamo per ordine e vediamo nel dettaglio quali sono i primi controlli su cui si focalizzeranno le verifiche.

In *primis* i controlli ricadranno sulla nomina del DPO: per chi era tenuto alla nomina e alla comunicazione, l'adempimento era da attuare entro il 25 maggio.

In *secundis* i controlli verteranno sul registro dei trattamenti: l'adozione doveva essere perentoriamente siglata entro il 25 maggio, magari anche certificata dalla data di ricezione dello stesso tramite pec.

Il registro dei trattamenti, lo ricordiamo, è uno strumento di fondamentale importanza, non solo per avere un quadro completo e aggiornato dei trattamenti all'interno di un'azienda o di un soggetto pubblico, ma anche per poter dimostrare e documentare, **dinanzi all'Autorità di controllo, la conformità dell'organizzazione alle norme del Regolamento Europeo**.

Anche se l'**obbligatorietà è prevista in casi specifici** (organismi con più di 250 dipendenti, quando il trattamento si basa su categorie particolari di cui all'art. 9 del Reg. o su trattamenti sistematici e non occasionali), il Garante ne ha da sempre consigliato l'utilizzo: "*come si potrebbe altrimenti dimostrare, senza tale ausilio di aver adottato tutte le misure necessarie a garantire il rispetto della normativa privacy, con il Registro infatti si ha la possibilità di sapere con esattezza quali trattamenti sono stati svolti in azienda, con quali modalità e tutte le misure di sicurezza adottate in riguardo*". Invitando quindi tutti i titolari del trattamento e i responsabili, **a prescindere dalle dimensioni dell'organizzazione**, a compiere i passi necessari per dotarsene.

In base all'art. 30, par.4 del Regolamento, per quanto suddetto, infatti: "*su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento* ***mettono il registro a disposizione dell'autorità di controllo***".

Ad ogni modo il Registro dei trattamenti sarà la base dell'attività ispettiva, il punto dal quale la Guardia di Finanza partirà per valutare le misure per la tutela della privacy messe in atto.

Altro aspetto importante è l'**obbligo formativo dei dipendenti**. Anch'esso, nei diversi aspetti, sarà oggetto di verifica della GdF (vedi articolo Fiscal Focus del 31.05.2018 GDPR: obbligo di formazione del personale).

Sintesi Verifiche ispettive: Durante gli accertamenti ispettivi da parte dell'Autorità Garante

privacy e della Guardia di Finanza (che ha rinnovato nel 2016 il protocollo di intesa con l'Autorità) gli step di verifica verteranno quindi:

- sul del registro trattamento dati;
- sulla nomina del DPO (se obbligatoria);
- sull'acquisizione del programma formativo, le dispense, i materiali erogati, il test finale;
- sull'**analisi del profilo** delle istruzioni agli incaricati al trattamento connesse all'accesso, alla consultazione delle banche dati, i livelli di autorizzazione e policy aziendali (ad esempio in materia di password aziendali e di videosorveglianza);
- sull'analisi delle misure organizzative e di protezione adottate;
- sui controlli sulle misure previste in caso di **data breach** (da intendere non come situazioni estreme ma come tutti quei casi di perdita accidentale e occasionale di dati, come il furto di un pc, di un hardisk e via di seguito) o in caso di valutazione di impatto.

Sanzioni – Sarà il Garante a decidere l'entità delle sanzioni, in base agli elementi raccolti durante la fase ispettiva della Guardia di finanza. Il Garante, secondo l'art. 83 del Regolamento, garantirà inoltre che essa sia **effettiva, proporzionata e dissuasiva**.

Ricordiamo, infatti, che il Garante Italiano detiene ancora il record per la più alta sanzione comminata, con la cifra di 11 milioni di euro, ottenuta sanzionando una società inglese e 4 aziende italiane, in violazione non solo della normativa antiriciclaggio, ma anche delle leggi sulla protezione dei dati personali.

Nel 2014 aveva emesso una sanzione di 1 milione di euro nei confronti di Google per la raccolta di immagini relative al servizio Google Street View. (Vedi articolo del 26 maggio 2018 GDPR: è febbre da Privacy).

È del **16 maggio 2018** la notizia (Ordinanza di ingiunzione nei confronti di Telecom Italia S.p.A.) **dell'applicazione della sanzione di 960 mila euro di sanzione alla Tim** per violazioni alla normativa sulla protezione dei dati personali e per un caso di data breach.

Autore: **Enza Mancuso**

Categorie: **Privacy > Disposizioni generali**

Via Alemanni 1 - 88040 Pianopoli (CZ) - ITALY
P.IVA 03426730796

E-mail: info@fiscal-focus.it