filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Che cosa ci insegnano le recenti decisioni del Garante Privacy su Eni Gas e Luce e TIM

20 Febbraio 2020
Laura Liguori, Giulio Novellini

Abstract
A distanza di più di un anno dalla piena applicazione del GDPR, il Garante ha applicato sanzioni elevate nei confronti di due operatori, contestando in dettaglio l'assenza o inadeguatezza delle procedure interne soprattutto in relazione ai database dei clienti gestiti dagli operatori per finalità di marketing.

L'attesa è terminata. A distanza di più di un anno dalla data di piena efficacia del Regolamento Generale sulla Protezione dei Dati Personali (GDPR) **arrivano in Italia le prime, significative, sanzioni del Garante per la protezione dei dati personali nei confronti di due operatori del settore utilities, Eni Gas e Luce e TIM**.

Dall'analisi dei due provvedimenti, ci sembra possano emergere alcune indicazioni fondamentali che possono guidare l'attività dei titolari di trattamento, dei consulenti e dei DPO presso i titolari (e, qualora nominati, i rispettivi responsabili del trattamento):

- **Istruttorie più complesse e globali**
  Il grado di dettaglio e di complessità delle ispezioni è sicuramente aumentato: nonostante in entrambi i casi il Garante sia partito da segnalazioni di interessati, l'istruttoria ha riguardato il complesso delle procedure interne degli operatori, il grado di consapevolezza dei flussi interni ed esterni relativi ai dati personali trattati dagli operatori, l'effettività dei controlli sui soggetti qualificati come responsabili del trattamento, l'esistenza di misure organizzative e tecniche documentate che comprovino il rispetto del GDPR. In una parola, l'accountability del titolare dei trattamenti;
- **L'importanza della Privacy by Design**
  In entrambi i casi, sono state sanzionate – tra le altre – le previsioni relative ai principi del trattamento (articolo 5) e privacy by design (articolo 25 GDPR). A sottolineare che quelle che – a prima vista – apparivano come norme di principio o addirittura (secondo alcuni) programmatiche, poiché sorrette da sanzioni pecuniarie, sono a tutti gli effetti obblighi normativi il cui mancato rispetto determina conseguenze rilevantissime per le aziende.
- **Procedure aziendali "by design"**

Entrambi i provvedimenti confermano l'erroneità di un modello di privacy aziendale di carattere "documentale" o "standard".Le procedure aziendali che le società avrebbero dovuto adottare sono esse stesse "by design": non si evincono dalla normativa, non sono richieste o previste specificamente dalla normativa applicabili, ma sono quelle necessarie al tipo di business condotto dalle società e che avrebbero dovuto essere adottate per evitare che si verificassero le violazioni contestate e sanzionate. Nessuno – a maggior ragione alla luce di queste decisioni – può più pensare che la compliance in materia di protezione dei dati personali possa limitarsi ad essere "documentale" o "standard".

- **Limitazione definitiva del trattamento e implementazione delle procedure appropriate**
  È stata disposta la limitazione definitiva del trattamento e la completa revisione e/o implementazione di alcune delle procedure aziendali. Il vero rischio – in caso di violazione del GDPR – oltre alla sanzione pecuniaria rilevante, è quello di trovarsi nell'impossibilità di trattare dati personali ed utilizzare data base per i quali il titolare potrebbe avere anche fatto degli investimenti, nonché quello di dover rivedere e/o implementare - sotto il controllo del Garante ed entro periodo di tempo dal medesimo stabilito - procedure aziendali necessarie per trattare i dati personali in conformità a quanto previsto dal GDPR;
- **Acquisti di liste da terzi**
  In caso di acquisti di liste di dati personali da terzi, non è sufficiente prevedere contrattualmente una garanzia da parte del terzo cedente di avere raccolto il consenso degli interessati alla comunicazione di dati a terzi per finalità di marketing. Se a maggior ragione non si acquista la lista dal titolare che ha raccolto tale consenso ma da un intermediario, è necessario accertarsi che quest'ultimo abbia raccolto l'ulteriore consento alla comunicazione a terzi. In altre parole, il consenso per comunicazioni a terzi non copre tutti i successivi passaggi, ma soltanto il primo;
- **Attivazione di utenze non richieste come trattamento illecito di dati personali**
  L'attivazione di contratti non richiesti (tradizionalmente sanzionata come pratica commerciale scorretta dall'Autorità Garante della Concorrenza e del Mercato) **può avere anche rilevanza sotto il profilo della protezione dei dati personali**. Qualora infatti tale attivazione avvenga a causa di una carenza di misure tecniche e organizzative che garantiscano la correttezza del trattamento e la qualità del dato, tale condotta è sanzionabile anche dal Garante ai sensi del GDPR;
- **Contitolarità**
  Non è escluso che, qualora un responsabile tratti dati personali acquisiti per proprio conto per finalità proprie, disattendendo le istruzioni del titolare, **il rapporto tra responsabile e titolare possa configurarsi** – in relazione a questi dati – **come contitolarità**. Ciò stante l'unitarietà dell'attività economica e l'impossibilità accertata di ritenere che il titolare non fosse al corrente dell'attività intrapresa dal responsabile di propria iniziativa.
- **Consenso per finalità di marketing e manifestazioni a premio**
  Subordinare la partecipazione a una manifestazione a premi al consenso per il trattamento di dati personali per finalità di marketing da parte degli interessati, non solo si pone in contrasto con il principio di libertà del consenso previsto dal GDPR, ma è altresì **in contrasto con il principio di gratuità della partecipazione alla manifestazione**, sancito dalla normativa in materia di manifestazioni a premi;
- **Legittimo interesse**
  L'utilizzo del legittimo interesse del titolare quale base giuridica del trattamento deve essere accompagnata da un attento bilanciamento tra i diritti degli interessati e le proprie aspettative circa il trattamento dei propri dati personali con l'interesse del titolare; tale bilanciamento deve essere adeguatamente documentato.

- **Data Breach**
  L'invio di dati personali (quali ad esempio la fattura e il traffico telefonico) a soggetti diversi dall'intestatario della linea telefonica si qualifica come violazione di dati personali (data breach): l'assenza di procedure idonee a garantire l'esattezza e l'integrità dei dati attraverso adeguate procedure interne, è sanzionata dal Garante; e
- **Fatturato considerato per il calcolo delle sanzioni**
  Il calcolo delle sanzioni ha tenuto conto delle varie circostanze aggravanti e attenuanti, ma vale la pena sottolineare come il calcolo del massimo edittale (che, ricordiamo, non è previsto dal GDPR, il quale si limita a prevedere che la sanzione amministrativa applicabile è fino a 20 milioni di Euro o, per le imprese, fino al 2% o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore) è avvenuto in entrambi i casi tenendo conto del fatturato della società oggetto di istruttoria e non del gruppo, così come definito dagli articoli 101 e 102 TFUE, come previsto dal Considerando 150 GDPR.

> **Le decisioni sono in linea con il piano dell'attività ispettiva deliberata a inizio 2018 (periodo nel quale hanno avuto inizio le attività istruttorie del Garante): vi si prevedeva, infatti, che fossero oggetto – tra gli altri – di ispezioni i trattamenti di dati personali effettuati da società per attività di telemarketing in relazione alle numerose segnalazioni pervenute all'Autorità. L'ultimo piano ispettivo di settembre 2019 si riferiva, tra gli altri, ai trattamenti effettuati mediante applicativi per la segnalazione di attività illecite (whistleblowing), ai programmi fedeltà, ai trattamenti di dati sanitari effettuati da società private. Sarà interessante seguire l'evoluzione dell'attività di enforcement da parte del Garante: soprattutto relativamente alla quantificazione delle sanzioni, l'assenza di linee guida sul calcolo delle medesime desta qualche perplessità e genera incertezza tra gli operatori.**

TAG: *privacy, GDPR, dati personali*
