GRUPPO DI LAVORO 29 - WP29

Le regole sul responsabile della protezione dati

Il 13 dicembre 2016 il Gruppo di Lavoro 29 (c.d. WP29) ha approvato una Linea guida "Responsabile per la protezione dei dati" (Data protection officer - Dpo) (oggi anche in italiano sul sito del Garante privacy). Si tratta di una figura cardine del nuovo regolamento, che troverà ampia applicazione anche in ambito sanitario.

L'articolo 37 del Regolamento 679/2016 stabilisce infatti che esiste l'obbligo del Dpo quando: «a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, oppure... c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9» (dati sensibili).

Pacifico quindi che tutte le strutture pubbliche - in quanto "organismi pubblici" - rientrano pacificamente nell'ambito applicativo della disciplina: quindi in data 25 maggio 2016 (piena efficacia del Regolamento) dovranno aver nominato il Dpo.

E le strutture private? Dalla mera lettura della norma sembra emergere che per i dati sensibili i criteri che devono esistere per far scattare l'obbligo della nomina del Dpo sono due: che il trattamento sia una delle "attività principali" e che lo stesso sia effettuato "su larga scala". Su tali due profili le Linee guida precisano quanto segue Sulla nozione di "attività principale" (punto 2.1.2)... l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare o dal responsabile. Per esempio, l'attività principale di un ospedale ("hospital" nella versione in inglese) consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente.

Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un Rpd.

Sulla nozione di "larga scala" il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti: trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività; ora, se si considera che il termine inglese "hospital" indica in generale le strutture sanitarie (sia pubbliche che private), sembra non esserci dubbio che tutte le case di cura, nonché case di riposo, Rsa ecc. siano tenute a nominare il Dpo.

Lo stesso Regolamento poi al considerando 91 esclude dal campo di applicazione il medico singolo, affermando che «Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato».

Alla luce di quanto sopra mi pare pacifico che case di cura e comunque strutture complesse devono nominare il Dpo, mentre il medico singolo non lo deve nominare.

Una zona d'ombra si apre invece per le strutture di media grandezza (es poliambulatorio o ambulatorio monospecialistici di ampie dimensioni): su queste aspettiamo lumi dal Garante privacy italiano.

Silvia Stefanelli
studio Stefanelli&Stefanelli


La garanzia del marchio Ce

Le regole sul responsabile della protezione dati

Trust da tassare con l'imposta di donazione