



Roma, 11/06/2018

- All'attenzione degli Uffici del Garante Privacy
Piazza di Monte Citorio n. 121
00186 ROMA

garante@gpdp.it

protocollo@pec.gpdp.it

dlps@gpdp.it

Oggetto: Obbligatorietà della nomina del DPO per sanitarie ed ortopedie. Istanza d'interpello.

Siamo con la presente a rivolgerci agli uffici dell'Autorità per la protezione dei dati al fine di poter contare su un parere autorevole in merito all'obbligatorietà della nomina di un Rappresentante della Protezione dei Dati per sanitarie ed ortopedie.

La richiesta nasce dalla difficoltà, pur seguendo i principi espressi dal GDPR e le precisazioni fornite successivamente dalle Authority nazionali, di riconoscere in modo chiaro la sussistenza delle condizioni poste alla base di tale nomina.

Per i **soggetti privati** come sanitarie ed ortopedia, infatti, l'obbligo sussisterebbe **solo in casi particolari**, quando cioè le attività principali («*core activities*») da essi svolte:

- richiedono monitoraggio regolare e sistematico degli interessati su larga scala; e/o
- consistono nel trattamento su larga scala di dati sensibili o giudiziari.

Inoltre, ai sensi del considerando 97 «*le attività principali* [«*core activities*», *n.d.a.*] del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria.

Su tali basi, si può affermare con certezza che per obblighi normativi D.Lgs. 46/97 concernenti i fabbricanti di dispositivi medici od i responsabili dell'immissione in servizio di tali dispositivi, **sanitarie ed ortopedie devono certamente praticare attività di monitoraggio ma non degli assistiti**, bensì dei dispositivi a questi forniti e che, le stesse, **trattano su larga scala data idonei a rivelare lo stato di salute ma non certo quale "core activities"**, essendo queste ultime riconducibili alla progettazione, fabbricazione e commercializzazione di dispositivi ortopedici.

Inoltre, le due qualificazioni «regolare» e «sistematico» valgono solo per il monitoraggio, non per il trattamento di dati particolari ed idonei a rivelare lo stato di salute, che potrà perciò non avere né regolarità né sistematicità.

La soggezione all'obbligo di designare il DPO, quindi, non è auto-evidente, nel caso di sanitarie ed ortopedie, pur ricorrendone, apparentemente, alcuni criteri, infatti, questi non si riferirebbero alle attività tipiche di tali imprese.

I Garanti europei sottolineano l'importanza di documentare, attraverso una analisi preliminare, azienda per azienda, la sussistenza delle caratteristiche di cui alla nomina del DPO medesimo, ma nel caso in specie, **tutte queste aziende, essendo soggette, perlopiù, all'erogazione di forniture pubbliche, risultano parimenti ed identicamente legate alle medesime procedure di erogazione dei servizi e dei dispositivi così come descritto nel DM 332/99 – regolamento dell'assistenza protesica** e, quindi, identicamente soggette ai medesimi trattamenti (prescrizione del dispositivo, scheda progetto, autorizzazione alla fornitura, misure e progetto del dispositivo, prova e consegna dello stesso, collaudo del bene e fatturazione elettronica).

Pertanto, l'attività tipica o primaria di una sanitaria od ortopedia può certamente essere generalizzata a caso specifico cui ricondurre l'intera popolazione di imprese private operanti sul territorio nazionale; **attività primaria che non è quella di trattare i dati particolari dei pazienti, ma di fornire dispositivi medici a questi ultimi**. Tuttavia, è evidente che questa attività presuppone necessariamente il trattamento dei dati sanitari dei pazienti che, diversamente, non potrebbe essere svolta.

Ma tale trattamento, che pure esiste, **non è core activity** perché, una volta descritto il caso e le sue implicazioni sanitarie in specifiche tecniche progettuali e di fabbricazione, non si esegue più nessun trattamento di tali dati particolari, non trattandosi di struttura sanitaria che deve verificare in termini di terapia, cura o riabilitazione gli esiti delle prestazioni erogate, essendo, tale compito in capo alle strutture sanitarie pubbliche che hanno prescritto il dispositivo ortopedico e che hanno trasferito a sanitarie ed ortopedie tali dati per l'esecuzione di una idonea progettazione.

Considerando ulteriori fattori così come ad avviso dei Garanti europei, la "regolarità" che, pure, non implica necessariamente "continuità", va detto che è vero che è regolare anche un monitoraggio periodico, dunque discontinuo, ma **nel caso di sanitarie ed ortopedie tale monitoraggio non è che sia ripetuto nel tempo** (cioè a determinati intervalli) **ma si sviluppa solo a giudizio ed al bisogno dell'assistito** che richieda successivi controlli e/o re-interventi sul dispositivo

Identicamente, «sistematico» non andrebbe inteso in senso temporale, ma in quella logica di: conforme a un sistema, a un piano, predefinito, metodico; in definitiva, non casuale né estemporaneo, caratteristiche che non presentano le attività di monitoraggio di sanitarie ed ortopedie sui dispositivi medici realizzati ed immessi in commercio.

Infine, riferendosi ad uno dei nodi più complessi e cioè il concetto di **larga scala**, sussiste un problema di quantificazione precisa che, i Garanti europei non hanno ben chiarito, neppure attraverso il ricorso ad alcuni esempi come quello di un professionista individuale per il quale non si potrebbe parlare di larga scala o, ancora della "piccola impresa familiare" che potrebbe non ricadere, anch'essa, nelle condizioni di larga scala.

Più controverso il caso della «media impresa», la cui attività di trattamento potrebbe essere su larga scala a seconda del caso di specie ma senza precisazioni in merito alla nozione di PMI, la quale, invece è precisata a livello europeo in base a parametri oggettivi indicati nella raccomandazione n. 2003/361/CE:

- è piccola impresa quella con meno di 50 dipendenti e fatturato totale annuo uguale o inferiore a 10 milioni di euro oppure un totale di bilancio annuo pari o inferiore a 10 milioni di euro;
- è microimpresa quella con meno di 10 dipendenti e fatturato totale annuo uguale o inferiore a 2 milioni di euro oppure un totale di bilancio annuo pari o inferiore a 2 milioni di euro.

Il concetto di impresa familiare (a prescindere dalle dimensioni) è basato invece, a livello europeo, su una definizione, di ampio e costante seguito, messa a punto a partire dal rapporto finale 2009 dell'Expert Group on Family Business.

Il collegamento del Regolamento con questi parametri dimensionali, ben consolidati in ambito societario, non trova, però, supporto esplicito nelle linee guida pubblicate che indicano criteri del tutto diversi, esclusivamente basati sul volume del trattamento anziché sulle dimensioni della struttura che vi procede:

- numero degli interessati coinvolti dal trattamento (o percentuale della popolazione di riferimento);
- volume dei dati personali trattati e/o loro ampiezza tipologica;
- durata del trattamento;
- contesto geografico di quest'ultimo.

Pertanto, ed alla luce delle considerazioni esposte, tenuto conto, altresì, dei chiarimenti già forniti dal Garante a Federfarma nel mese di marzo u.s. relativamente alla non sussistenza dell'obbligo per le farmacie di designare il Dpo in quanto le stesse non effettuano trattamenti su larga scala; le scriventi, ritenendo che le attività di trattamento siano sostanzialmente identiche per tutte le sanitarie ed ortopedie perché legate ad un sistema regolamentato, indipendentemente dalla loro specializzazione e/o dimensione organizzativa, e non trovando nel GDPR e nelle successive precisazioni di cui alle Authority nazionali, chiari ed evidenti rimandi a requisiti di trattamento di dati personali e particolari che supportino la necessità di nominare un Responsabile della Protezione dei Dati (DPO), ritengono che sanitarie ed ortopedie debbano essere escluse da quest'obbligo ma, data l'incertezza della materia, sono a chiederne parere all'Autorità in indirizzo di cui auspicano un sollecito riscontro.

Ringraziando per l'attenzione si formulano i nostri migliori saluti.

Per ANTOI : Silvia Guidi e Provvido Mazza

Per Assortopedia : Alessandro Maggi

Per CIDOS : Carlo Landi

Per FIOTO : Marco Laineri Milazzo