aris
Trimestrale dell'Associazione Religiosa Istituti Socio-Sanitari

SANITA'

Anno XXIX • Numero 1 • Marzo 2017

12 Anni Insieme

Assemblea Elettiva

Anno XXIX • Numero 1 • Marzo 2017 • Poste Italiane SpA • Spedizione in abbonamento postale 70% • DCB Roma

Anno XXIX – n. 1
Marzo 2017

Direttore Responsabile:
Mario Bonora

Comitato Scientifico:
Dr. Domenico Galbiati (responsabile)
Dott.ssa Maria Teresa Iannone
Prof. Salvino Leone
Dott. Mario Mazzoli

Redattore Capo:
Mario Ponzi

Vicecaporedattore:
Maria Rita Gentile

Redazione:
Raffaele D'Ari,
Gianni Cristofani,
Mauro Mattiacci,
Alfredo d'Ari
Nevio Boscariol

Segretario di Redazione:
Massimo Scafetti

Progetto grafico e ricerca iconografica:
Tipolitografia Empograph

Foto:
Archivio ARIS

Volumi e pubblicazioni:
Rizzoli, Skira–Corriere della Sera, Milano;
I classici dell'Arte; Complesso Integrato Columbus – Roma; Congregazione dei Figli dell'Immacolata Concezione – Roma

Stampa:
Tipolitografia Empograph
Via Venezia Tridentina, 1
00010 Villa Adriana (Roma)

Direzione, Redazione, Amministrazione:
P.zza SS. Giovanni e Paolo, 13
00184 Roma
Tel. 067726931 – Fax 0677269343

Pubblicità:
P.zza SS. Giovanni e Paolo, 13
00184 Roma
In attesa di autorizzazione
del Tribunale di Roma

Finito di stampare nel mese di marzo 2017

SOMMARIO

NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY: COME PREPARARSI

di Tania Caputo*

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento 2016/679 General Data Protection Regulation (GDPR). Entrato in vigore il 25 maggio 2016, prevede la piena applicazione entro il 25 maggio 2018.

I principali vantaggi di una disciplina armonizzata all'interno dell'Unione Europea sono molteplici: una più adeguata ed uniforme protezione dei dati personali, la garanzia della corretta libera circolazione dei dati all'interno dell'Unione, l'allineamento dei termini utilizzati per definire l'impianto normativo necessario per la tutela dei dati, la disciplina stringente di istituti che oggi sono presenti solo per alcuni tipi di dati (è il caso dell'obbligo di comunicazione del Data Breach attualmente previsto solo per il Dossier Sanitario), la definizione delle Autorità di Controllo, la tutela dei dati che vengono trasmessi al di fuori dell'Unione Europea, la garanzia della portabilità del dato ed il c.d. diritto all'oblio. Il principale riflesso di questi aspetti positivi, si ripercuote sull'impostazione stessa del sistema privacy italiano: passeremo da un sistema attualmente burocratico ad un sistema di gestione privacy basato sui principi della "privacy by design" e "privacy by default"[1]. Ciò

Tabella 1

Definizione GDPR in inglese	Definizione GDPR (traduzione ufficiale in italiano)	Correlazione all'attuale Codice Privacy
Data Subject	Interessato	Interessato
Data Controller	Titolare del Trattamento dei dati	Titolare del Trattamento dei dati
Data Processor	Responsabile del Trattamento dei dati	Responsabile del Trattamento dei dati
Data Protection Officer	Responsabile della Protezione dei dati	Non previsto
Person Authorised to	Persona autorizzata al Trattamento dei dati	Incaricato al Trattamento dei dati
Supervisory Authority	Autorità di Controllo	Garante per la Protezione dei dati
Personal Data	Dato Personale	Dato Personale
Data concerning health	Dati riguardanti la salute	Dati riguardanti la salute
Special categories of personal data	Categorie particolari di dati	Dati Sensibili (con alcune modifiche alla definizione)
Data Breach	Violazione dei dati	Data Breach (previsto solo per il Dossier Sanitario e per i fornitori di servizi di comunicazione elettronica accessibili al pubblico)
Right to be erase (right to be forgotten)	Diritto alla cancellazione (diritto all'oblio)	Non previsto
Data Portability	Portabilità del dato	Non previsto
Prior consultation	Consultazione preventiva	Verifica preliminare

1 - L'art. 25 del GDPR traduce questi concetti con la frase "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita". Mentre il primo concetto fa riferimento alla valutazione della probabilità dei rischi e della gravità per i diritti e le libertà dei singoli, il secondo ricorda la necessità di trattare in modo predefinito solo i dati personali utili per le finalità previste e per il periodo strettamente necessario a tali fini.

comporta una revisione complessiva degli strumenti oggi previsti dalle strutture sanitarie con l'adozione di un approccio strutturato ed armonizzato. Particolare attenzione dovrà essere dedicata agli aspetti informatici, data la crescente dematerializzazione della documentazione sanitaria.
In attesa delle numerose previsioni delle quali attendiamo l'emanazione nel corso del 2017 - alcune già pubblicate dal Working Party 29[2] - è opportuno iniziare a muoversi nel nuovo assetto previsto dal GDPR. Il lavoro che attende la struttura sanitaria è particolarmente complesso e delicato vista la natura del dato trattato e vista l'assenza di figure specializzate già attive nei nostri Enti (sono davvero poche le strutture che hanno una figura esperta del settore privacy).

Per poter entrare gradualmente nel GDPR, è opportuno allineare la terminologia utilizzata[3]. La tabella seguente mostra la definizione europea (in inglese ed in italiano) e la relativa corrispondenza rispetto all'attuale impianto normativo (Tabella1)
Ma non cambia solo la terminologia. Uno dei principali strumenti che ad oggi il Codice della Privacy non prevede, è la figura del Data Protection Officer (DPO). Dopo soli sei mesi dalla pubblicazione del GDPR, il Working Party 29 ha adottato, in data 13 dicembre 2016, le linee guida di dettaglio per stabilire chi debba obbligatoriamente designare il DPO, quale sia la sua posizione nell'organizzazione ed i compiti che debba svolgere. Già il GDPR pareva chiaro rispetto alle strutture sanitarie: è obbligato a nominare il DPO chi ha nel proprio "core" la processazione su larga scala di categoria di dati "speciali" o di dati legati agli aspetti penali. L'aver indicato il termine "speciale" ci riporta direttamente a tutti quei dati che oggi chiamiamo sensibili ed in particolare quei dati idonei a rivelare lo stato di salute. La struttura sanitaria, per eccellenza, tratta dati a carattere sanitario e rientra quindi tra gli Enti che devono obbligatoriamente nominare un DPO[4].
Appare utile un primo inquadramento dell'ambito della definizione di "dato sensibile", confrontando l'attuale Codice della Privacy con il GDPR. Le tematiche più delicate, oggi disciplinate da provvedimenti specifici o senza una disciplina specifica, vengono incluse nelle nuove de-

Tabella 2

Codice della Privacy - Art. 4 punto d) Definizioni	GDPR - Art. 9 Processing of special categories of personal data
Dati personali idonei a rivelare:	Personal data revealing:
l'origine razziale ed etnica	racial or ethnic origin
le opinioni politiche	political opinions
le convinzioni religiose, filosofiche **o di altro genere**	religious or philosophical beliefs
l'adesione a partiti, sindacati,	trade union membership
associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale	
i dati personali idonei a rivelare lo stato di salute	**genetic data, biometric data,** data concerning health
e la vita sessuale	data concerning sex life or **sexual orientation**

2 - Il Working Party 29 è un organo indipendente e consultivo dell'Unione Europea, costituito ai sensi dell'art. 29 della Direttiva 95/46/EC. E' composto dai Rappresentanti dei Garanti per la protezione dei dati degli stati Membri ed ha il compito di contribuire all'omogenea applicazione delle norme nazionali di attuazione della Direttiva EU che tutela i dati.

3 - La traduzione ufficiale del GDPR presenta alcuni errori che, nella presente analisi, vengono superati con le diciture corrette.

4 - Le Linee Guida del WP29 citano espressamente l'Ospedale come Ente che deve nominare obbligatoriamente un DPO. Viene inoltre confermato che i dati trattati continuativamente da un Ospedale si qualificano come trattamenti su larga scala.

Tabella 3

Data Protection Impact Assessment (DPIA)	Valutazione dell'impatto relativo al Trattamento da effettuare. Deve essere eseguita prima di procedere al trattamento stesso.
Data Portability (Portabilità dei dati)	Il diritto dell'interessato alla portabilità dei dati comporta analisi di fattibilità tecnica poiché i dati sanitari hanno strutturazione complessa e non compatibile a priori con i formati in uso presso altre strutture sanitarie. In merito, il Working Party 29 ha adottato – in data 13 dicembre 2016 – le linee guida per garantire tale diritto.
Records of processing activities (Registro delle attività di Trattamento)	Ogni Titolare e ogni Responsabile del Trattamento dei dati deve tenere un registro con una serie di informazioni specifiche. Sono esonerati gli Enti con meno di 250 dipendenti a meno che il trattamento riguardi categorie particolari dei dati. Tutte le strutture sanitarie sono quindi tenute all'adempimento del Registro.
Cross-border processing (Trasferimento transfrontaliero)	Strutturazione di una gestione del trasferimento che prevede l'adeguata tutela del dato con verifica delle Binding Corporate Rules (BCR) o rispetto del Privacy Shield

finizioni, aumentando il livello di tutela offerto al cittadino (Tabella 2).

Il GDPR prevede inoltre altri strumenti che attualmente il nostro sistema non conosce in modo approfondito, sintetizzabili nella Tabella 3.

Come è possibile rilevare da quanto descritto, il programma di allineamento al GDPR richiede tempo e risorse multidisciplinari poiché le attività richieste impattano su aspetti organizzativi, legali ed informatici.

I numerosi temi da affrontare potranno essere programmabili in due step:

- Entro il 31/12/2017: formazione sul GDPR per il gruppo di lavoro multidisciplinare, definizione di un Modello Organizzativo del Sistema Privacy (c.d. MOSP), stesura del Data Privacy Impact Assessment (DPIA), stesura del Privacy Program e del Regolamento del Data Protection Officer.
- Entro il 30/04/2018: aggiornamento delle procedure e dei documenti privacy, strutturazione degli strumenti tecnici richiesti dal GDPR, test sulla tenuta del sistema privacy, formazione estesa a tutti i dipendenti e collaboratori.

L'impegno richiesto deve essere finalizzato a due obiettivi primari:

- Tutelare i dati dei pazienti in modo corretto e secondo la normativa vigente, ricordando che si tratta di dati costituzionalmente garantiti.
- Evitare le pesanti sanzioni previste dal GDPR. Su questo aspetto appare utile ricordare che il sistema sanzionatorio previsto dal GDPR prevede sanzioni amministrative pecuniarie fino a 10 o 20 milioni di Euro (a seconda del tipo di violazione) elevabili al 2% o 4% (a seconda del tipo di violazione) del fatturato annuo mondiale dell'esercizio precedente qualora tale secondo parametro sia maggiore della sanzione base. La severità delle sanzioni impone una riflessione sull'importanza che l'Europa assegna ai diritti legati al trattamento dei dati e sulla chiara volontà di punire le grandi società dell'informazione che violano agevolmente la normativa della privacy dato l'impatto economico non rilevante delle sanzioni previste.

**Responsabile Affari Legali e Societari Poliambulanza di Brescia*

Focus on...Data Protection Officer (DPO)
Le Linee Guida del Working Party Article 29 (WP29)

La nuova figura introdotta dal GDPR identifica il cuore dei nuovi adempimenti legali delle grandi organizzazioni, avendo sostanzialmente un ruolo cruciale per facilitare la compliance normativa.
E' obbligatoria la nomina del DPO in tre casi:

a) quando il dato è trattato da una autorità o ente pubblico (definizioni da ricondurre alle specifiche leggi nazionali, con inclusione degli enti privati che svolgono funzioni o compiti pubblici);
b) quando le attività "core" (cioè primarie) consistono nel trattamento di dati su larga scala (numero e volume dei dati trattati, durata del trattamento, estensione geografica del trattamento) o in modo regolare/sistematico (trattamento costante, regolare e organizzato).
c) quando l'attività "core" consiste nel trattamento su larga scala di categorie speciali di dati o dati relativi a condanne penali o reati.

Il WP29, nelle esemplificazioni, specifica che l'Ospedale ha nelle sue attività "core" la fornitura di Servizi Sanitari che non possono quindi prescindere dal trattamento dei dati sanitari dei pazienti[5], rendendo quindi obbligatoria la nomina del DPO. Specifica nuovamente questo obbligo quando esemplifica il trattamento su larga scala[6], escludendo invece il trattamento dei dati sanitari operati da un singolo medico (per esempio nella propria attività libero professionale esterna alla struttura sanitaria).
Le Linee Guida del WP29 dedicano particolare attenzione all'esperienza e alla capacità del DPO. Nello specifico, evidenziano la necessità di una professionalità con esperienza nella normativa sulla protezione dei dati (sia nazionale che europea) e l'abilità per poter gestire tutte le attività affidata dall'art. 39 del GDPR, cioè:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento

Il DPO deve essere coinvolto e consultato in ogni decisione relativa alla protezione dei dati, deve avere sufficiente tempo per adempiere ai propri compiti, deve essere supporto in termini finanziari, strutturali e organizzativi, deve poter accedere ai servizi coinvolti nel trattamento dei dati, deve essere formato ed aggiornato sulle tematiche del trattamento dei dati e deve disporre, specie nel caso di grandi organizzazioni, di un team con il quale poter condividere le attività. Deve inoltre agire in modo indipendente ed in assenza di conflitti di interesse.
Una nuova figura che, come strutture sanitarie, ci abitueremo presto a conoscere e che avrà un obiettivo primario: coinvolgerci attivamente nel nuovo mondo della privacy "all'europea".

5 ...the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patient's health records. Therefore, processing these data should be one of any hospital's core activities and hospital must therefore designate DPOs".

6...processing of patient data in regular course of business by a hospital..."