Regione Puglia
OSPEDALI RIUNITI
Azienda Ospedaliero – Universitaria
FOGGIA

DELIBERAZIONE DEL DIRETTORE GENERALE

Nominato con Deliberazione della Giunta Regionale n. 805 del 17/4/2015

n. 168 del 12 APR 2017

OGGETTO

Nomina del Responsabile della Protezione dei Dati - Data Protection Officer (DPO) - ai sensi del considerando art. 37 del Regolamento UE 679/2016.

Struttura proponente	Controllo di gestione

Documenti integranti il provvedimento:

Descrizione Allegato	n. pag.

☑ **Dichiarazione di immediata esecutività**

Spese previste	
Conto Economico n.	
Descrizione conto economico	
Bilancio	
Dirigente	Dott.Cordisco

Destinatari dell'atto per conoscenza

☑ Direzione Amministrativa	☑ Direzione Sanitaria
☐ Struttura Controllo di Gestione	☐ Struttura Economico-Finanziaria
☑ Struttura Affari Generali e Tutela della Privacy	☐ Struttura Politiche del Personale
☑ Altro (specificare) interessato	

La presente Deliberazione, tenuto conto delle fonti normative relative alla disciplina della privacy ovvero della tipologia degli atti allegati, è pubblicata con le seguenti modalità:

- ☐ solo frontespizio
- ☑ integrale
- ☐ solo deliberazione

Visto il D. Lgs n. 196/2003 (Codice in materia di protezione dei dati personali), entrato in vigore in data 01.01.2004, contenete importanti innovazioni sulla riservatezza delle comunicazioni elettroniche, alla luce dei chiarimenti del Garante per la Protezione dei dati Personali e della Direttiva UE 2000/58;

Evidenziato che la finalità della normativa citata è quella di garantire che il trattamento dei dati personali, sensibili e giudiziari si svolga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, sensibili e giudiziari;

Dato atto che la tutela dei diritti sopra citati, secondo la volontà del legislatore nazionale, deve essere assicurata nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte dei Responsabili e degli incaricati addetti al trattamento dei dati, nonché per l'adempimento degli obblighi di Legge da parte del Titolare del Trattamento;

Considerato che la Regione Puglia, con l'art. 39, comma 14, della L.R. n. 4/2010 ha previsto, tra l'altro, che le ASL, le AOU, gli IRCCS e le strutture private accreditate individuano, al proprio interno, una funzione dedicata alla gestione delle problematiche relative al trattamento dei dati personali e sensibili al fine di garantire l'attuazione di quanto contenuto nel D. Lgs. n. 196/2003 e nel Regolamento Regionale n. 5/2006;

Rilevato che il Garante Privacy, nelle Linee Guida in materia di Dossier Sanitario in allegato A alla deliberazione del 4 Giugno 2015, dispone che i Titolari del trattamento individuino al loro interno una figura di Responsabile della Protezione dei Dati che svolga il ruolo di referente con il Garante (*c.d.* DPO - Data Protection Officer), anche in relazione ai casi di cosiddetta "data breach" (violazione dei dati personali);

Preso atto che il nuovo Regolamento Privacy UE 679/2016 è entrato in vigore il 24 maggio 2016 e prevede la designazione obbligatoria di un Responsabile della Protezione dei dati nelle Amministrazioni ed Enti Pubblici;

Richiamate le Deliberazioni del Direttore Generale:

- DDG n. 75 del 21 febbraio 2017 avente ad oggetto: "Decreto Legislativo 30 giugno 2003, n. 196. "Codice in materia di protezione dei dati personali" e Regolamento Europeo Privacy UE 2016/679 del 27 Aprile 2016: Individuazione e nomina dei responsabili ed Incaricati del trattamento dei dati e degli Amministratori di Sistema";
- DDG n. 64 del 11 febbraio 2017 avente ad oggetto: "Regolamento per l'utilizzo e la gestione delle risorse strumentali informatiche e telematiche aziendali- approvazione";
- DDG n. 76 del 21 febbraio 2017 avente ad oggetto: "Adozione del Regolamento per le richieste di oscuramento e de-oscuramento dei dati con relativi allegati e dei nuovi modelli di Informativa e Consenso Privacy per il trattamento dei dati personali in conformità al D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" e s.m.i.";

Atteso che il considerando art. 37 del nuovo Regolamento Europeo sulla Protezione dei dati personali, nella versione della Commissione Europea, elenca i compiti del DPO (Responsabile della protezione dei dati personali) come di seguito riportati:

a) informare e consigliare il Titolare del trattamento in merito agli obblighi derivanti dal Regolamento e conservare la documentazione relativa a tale attività e alle risposte ricevute;
b) sorvegliare l'attuazione e l'applicazione delle politiche del Responsabile del trattamento o dell'incaricato del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e gli audit connessi;
c) sorvegliare l'attuazione e l'applicazione del Regolamento, con particolare riguardo ai requisiti concernenti la protezione fin dalla progettazione, la protezione di default, la sicurezza dei dati, l'informazione dell'interessato e l'esercizio dei diritti riconosciuti dal Regolamento;
d) garantire la conservazione della documentazione inerente la Privacy Aziendale;
e) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate (Data Breach);
f) controllare che il responsabile del trattamento o l'incaricato del trattamento effettui la valutazione d'impatto sulla protezione dei dati e richieda l'autorizzazione preventiva o la consultazione preventiva quando prevista;
g) controllare che sia dato seguito alle richieste dell'Autorità di Controllo e, nell'ambito delle sue competenze, cooperare con l'Autorità di Controllo di propria iniziativa o su sua richiesta;
h) fungere, da punto di contatto, per l'Autorità di Controllo per questioni connesse al trattamento e, se del caso, consultare l'Autorità di Controllo di propria iniziativa;

Considerata l'esperienza già acquisita e la competenza giuridica dimostrata dal Dirigente della Struttura Dipartimentale Affari Generali e Tutela della Privacy nella persona della dott.ssa Laura Silvestris;

Dato atto che sino ad oggi la dott.ssa Laura Silvestris ha assicurato, in modo efficiente ed efficace, tutte le attività obbligatorie previste per legge e sono in itinere altri adempimenti curati sempre dalla stessa Dirigente;

Acquisito il parere favorevole del Direttore Amministrativo e del Direttore Sanitario, ciascuno per la parte di rispettiva competenza;

DELIBERA

per le ragioni precisate in narrativa che qui si intendono integralmente riportate e confermate

1. di nominare la dott.ssa Laura Silvestris, Dirigente della Struttura Dipartimentale Affari Generali e Tutela della Privacy, Responsabile della Protezione dei Dati (DPO – Data Protection Officer), anche in relazione ai casi di "Data Breach" (violazione dei dati personali), come richiesto dal Garante Privacy nel Provvedimento n. 331 del 4 giugno 2015 e relativi allegati A/B alla deliberazione stessa;

2. di dare atto che per effetto del presente provvedimento non sono previsti oneri finanziari a carico del bilancio all'Azienda;

3. di notificare il presente provvedimento al Dirigente interessato, dott.ssa Laura Silvestris.

Il presente provvedimento, non essendo soggetto al controllo previsto dalla vigente normativa, è esecutivo ai sensi di legge.

Il Dirigente proponente
dott. Giuseppe Cordisco

Il Direttore Sanitario
dott.ssa Laura Liliana Moffa

Il Direttore Amministrativo
dott. Michele Ametta

Il Direttore Generale
dott. Antonio Pedota

CERTIFICATO DI PUBBLICAZIONE

Il presente atto viene posto in pubblicazione in data odierna sull'Albo Pretorio informatico dell'Azienda Ospedaliero-Universitaria "Ospedali Riuniti" di Foggia.

Foggia, 12 APR 2017

F.to IL FUNZIONARIO ADDETTO

Allegato 1 al Provvedimento del 2 luglio 2015

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal **Provvedimento del 2 luglio 2015**, le amministrazioni pubbliche sono tenute a comunicare al Garante all'indirizzo: **databreach.pa@pec.gpdp.it** le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. *p* del Codice) di cui sono titolari.

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Amministrazione titolare del trattamento

Denominazione o ragione sociale _____

Provincia _____ **Comune** _____

Cap _____ **Indirizzo** _____

Nome persona fisica addetta alla comunicazione _____

Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

Allegato 1

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro :

Allegato 1

Dispositivo oggetto della violazione

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di *backup*
- ☐ Documento cartaceo
- ☐ Altro :

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ N. _____ persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
- ☐ Dati relativi a minori
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro :

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

Allegato 1

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il

☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Violazioni di dati personali *(data breach)*

Gli adempimenti previsti

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali ha adottato una serie di provvedimenti che introducono per amministrazioni pubbliche e aziende l'obbligo di comunicare i casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o comunque trattati.
La scheda, che ha mere finalità divulgative, riassume i casi finora esaminati.

SOCIETA' TELEFONICHE E INTERNET PROVIDER

Art. 32-*bis* del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]

- **L'obbligo di comunicazione al Garante** *(mediante un apposito modello di comunicazione)* riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli *internet point*, le reti aziendali).
- In caso di violazione dei dati personali, società di tlc e Isp **devono**:
  a. **entro 24 ore** dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
  b. **entro 3 giorni dalla scoperta,** informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
- La comunicazione agli utenti **non è dovuta** se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un **inventario** costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE (art. 162-*ter* del Codice in materia di protezione dei dati personali)**
  - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
  - per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
  - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

BIOMETRIA

Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]

- **Entro 24 ore** dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

DOSSIER SANITARIO ELETTRONICO

Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]

- **Entro 48 ore** dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

AMMINISTRAZIONI PUBBLICHE

Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]

- **Entro 48 ore** dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

Per approfondimenti, consultare i provvedimenti pubblicati sul sito: www.garanteprivacy.it