DELIBERAZIONE DEL DIRETTORE GENERALE

Nominato con Deliberazione della Giunta Regionale n. 1640 del 17/10/2017

n. 409 del 18 maggio 2018

OGGETTO

Adozione di Regolamento in materia di *data-breach* per la gestione delle violazioni dei dati personali, ex art. 33 del Regolamento UE 2016/679.

Struttura proponente	SSD AFFARI GENERALI E TUTELA DELLA PRIVACY

Documenti integranti il provvedimento:

Descrizione Allegato	n. pag.
Regolamento	6
Allegato n. 1	4
Allegato n. 2	2

☑ **Dichiarazione di immediata esecutività**

Spese previste	
Conto Economico n.	
Descrizione conto economico	
Bilancio	
Dirigente	Dott.ssa Laura Silvestris

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) Direttori e Dirigenti di Struttura	

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

Premesso che:

- dal 1 gennaio 2004 è in vigore il decreto legislativo 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali;
- in data 24 maggio 2016 è entrato in vigore il Regolamento UE 2016/679, pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, il quale abroga la direttiva 95/46/CE;
- il cosiddetto Pacchetto Europeo protezione dei dati troverà applicazione negli Stati Membri dal 25 maggio 2018;

Evidenziato che il succitato Regolamento definisce:

- all'art. 4 c.12 la «Violazione dei dati personali» (data breach) quale violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- agli artt. 33 e 34 le modalità per la "Notifica di una violazione dei dati personali all'autorità di controllo";

Richiamate le seguenti deliberazioni del Direttore Generale:

- DDG n. 75 del 21 febbraio 2017 - 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 - Regolamento per l'utilizzo e la gestione della risorse strumentali informatiche e telematiche aziendali. Approvazione;
- DDG n. 76 del 21 febbraio 2017 - Regolamento per le richieste di oscuramento e de-oscuramento dei dati con relativi allegati e dei nuovi modelli di informativa e consenso privacy;
- DDG n. 168 del 12 aprile 2017 - Nomina del Responsabile della Protezione dei Dati - Data Protection Officer (DPO) - ai sensi del considerando art. 37 del Regolamento UE 679/2016;
- DDG n. 117 del 16 marzo 2017 - Codice della Privacy - Adempimenti ex D. Lgs. n. 196/2003 e s.m.i. – Recepimento delle Linee guida per i trattamenti dei dati personali nell'ambito delle sperimentazioni cliniche di medicinali;
- DDG n. 125 del 20 marzo 2017 - Regolamento accesso agli atti ed alla documentazione amministrativa e disciplina dell'accesso civico;
- DDG n. 563 del 29 novembre 2017 - Nomina del responsabile del procedimento di conservazione dei documenti informatici e gestione dei flussi documentali ai sensi dell'art. 44, comma 1 - bis del D.Lgs n. 82/2005, del Responsabile e del Referente del Protocollo Informatico e del Responsabile esterno del trattamento dei dati, ai sensi del D. Lgs. 198/2003 ed in osservanza del nuovo Regolamento Privacy (U.E.) n. 679/2016;
- DDG n. 402 del 31 luglio 2017 "Adozione del Regolamento per impianti di videosorveglianza ex D.Lgs n. 196/2003 e Regolamento UE 679/2016";

Dato atto che una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata

della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata;

Rilevata la necessità di adeguarsi al nuovo adempimento imposto dal Regolamento UE 2016/679, proponendo un Regolamento che definisca le modalità per la notificazione di eventuali violazioni di dati personali *(c.d. data breach);*

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

DELIBERA

1. di adottare il Regolamento aziendale per la segnalazione di violazioni di dati personali, parte integrante e sostanziale del presente atto, ai sensi dell'art. 33 del Regolamento UE 2016/676;

2. di disporre che il presente provvedimento venga pubblicato nell'albo pretorio online e a tutti i Dirigenti titolari di Struttura dell'AOU di Foggia.

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

Il Dirigente Proponente
dott.ssa Laura Silvestris

Il Direttore Sanitario
dott.ssa Laura Liliana Moffa

Il Direttore Amministrativo
dott. Michele Ametta

Il Direttore Generale
dott. Vitangelo Dattoli

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, 22 MAG 2018

F.to IL FUNZIONARIO ADDETTO
Vincenzo Sabatino

REGOLAMENTO IN MATERIA DI DATA BREACH

Regolamento UE 2016/679 in materia di violazione di dati personali

SSD Affari Generali e Tutela della Privacy

REGOLAMENTO IN MATERIA DI *DATA BREACH*

Indice

ALLEGATI:

Allegato n. 1: Modello segnalazione data breach PA

Allegato n. 2: Modello interno segnalazione violazioni

Articolo 1 – Significato di Data Breach

Il Regolamento UE 2016/679 all'articolo 4 c. 12) intende per «violazione dei dati personali»:la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Articolo 2 – Notifica della violazione

In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Ciascun Responsabile del trattamento informa il Titolare del trattamento, anche per il tramite del Responsabile della protezione dei dati, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Titolare, con il supporto del Responsabile della protezione dei dati, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. A tal fine è reso disponibile un modello per la segnalazione, predisposto dal Garante, che si allega al presente regolamento (Modello segnalazione data breach PA). La notifica è effettuata tramite posta elettronica certificata del Titolare del trattamento con l'invio del modello per la segnalazione all'indirizzo e-mail databreach.pa@pec.gpdp.it.

Articolo 3 – Comunicazione all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni:

a) la natura della violazione dei dati

b) i dati di contatto del Responsabile della protezione dei dati
c) le possibili conseguenze della violazione
d) le misure adottate o di cui si propone l'adozione per porvi rimedio.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Articolo 4 – Determinazioni del Garante

Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui sopra è soddisfatta.

Articolo 5 – Valutazione dei Rischi

Nel caso di violazione dei dati personali il Titolare del trattamento procede con una valutazione complessiva dell'impatto sui diritti e libertà degli interessati in considerazione della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento.

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

a. se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
b. se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
c. se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
d. in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;

e. se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Il Titolare, con il supporto del Responsabile della protezione dei dati, verifica se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali ed informa tempestivamente il Garante e l'interessato, se del caso.

Articolo 6 – Azioni conseguenti

A seguito della valutazione preliminare della violazione, il Titolare del trattamento con il supporto del Responsabile della protezione dei dati, adotta una le seguenti azioni:

a) se dalla violazione risulta probabile che possano derivare rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data-breach* al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento;
b) se dalla violazione risulta probabile che possano derivare elevati rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data-breach* al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento e alla comunicazione della violazione ai soggetti interessati ai sensi dell'art. 34 del Regolamento UE 2016/679;
c) ove non risulti probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento non procede con le notifiche e comunicazioni di cui ai p.ti a) e b).

Pertanto, il Titolare del trattamento è esentato dalla notifica della violazione solo se è in grado di dimostrare al Garante che il *data-breach* non presenta rischi per i diritti e le libertà fondamentali delle persone fisiche interessate.

Articolo 7 – Modalità operative

Ogni Responsabile di Struttura Complessa, Semplice Dipartimentale e Semplice, in quanto Responsabile del trattamento, per ambito di competenza, ha l'obbligo di segnalare senza ingiustificato ritardo, entro 24 ore, la violazione dei dati rilevata ai soggetti di seguito elencati:

- Titolare del trattamento
- Responsabile della protezione dei dati
- Direzione Sanitaria
- Direzione Amministrativa.

La segnalazione, in prima istanza, può essere effettuata in qualsiasi forma, anche per le vie brevi e successivamente formalizzata tramite invio di posta elettronica o atto da protocollare. Ai fini dell'osservanza dei tempi imposti dal Regolamento Ue 2016/679, il Titolare del trattamento dei dati, provvederà a convocare, non oltre 24 ore dalla rilevazione della violazione, una riunione con i soggetti di seguito elencati:

- Responsabile della protezione dei dati
- Responsabile dei Sistemi Informatici
- Responsabile del trattamento dell'Unità interessata dal data-breach.

Il Responsabile della protezione dei dati ha facoltà di convocare altri soggetti ritenuti necessari per la valutazione della gravità della violazione dei dati.

Il Responsabile della protezione dei dati è tenuto a documentare l'intera attività istruttoria, acquisendo tutte le informazioni necessarie per la registrazione dell'evento e per la notificazione al Garante, ove necessario. A conclusione della valutazione della violazione, il Responsabile della protezione dei dati predispone un verbale, sottoscritto da tutti i convenuti e protocollato, che sarà inoltrato al Titolare del trattamento per i conseguenti adempimenti di cui agli artt. 2 e 3 del presente Regolamento.

Articolo 8 – Registro delle violazioni

Il Titolare del trattamento documenta le violazioni dei dati in apposito registro elettronico da esibire in caso di accertamento ispettivo dell'Autorità.

Il registro delle violazioni è custodito dal Responsabile della protezione dei dati con la massima diligenza e nell'osservanza del Regolamento UE 2016/679.

Articolo 9 – Sanzioni

Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma del Regolamento UE 2016/679, ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto di uno Stato membro, con obiettivi statutari di pubblico interesse, e che siano attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto al Garante, esercitare il diritto a un ricorso giurisdizionale per conto degli interessati o esercitare il diritto di ottenere il risarcimento del danno per conto degli interessati se quest'ultimo è previsto dal diritto degli Stati membri.

Il Titolare del trattamento o il Responsabile del trattamento è tenuto a risarcire i danni cagionati ad una persona da un trattamento non conforme al Regolamento UE 2016/679 ma è esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

La violazione delle disposizioni contenute nel Regolamento 2016/679 è soggetta a sanzioni amministrative pecuniarie fino a € 10.000.000,00.

Articolo 10 – Norma finale

Per quanto non espressamente previsto nel presente Regolamento si fa rinvio al Regolamento UE 679/2016 e successive regolamentazioni.

Il Titolare del trattamento si riserva di modificare e integrare il presente Regolamento, ove ritenuto necessario, anche alla luce di eventuali successive innovazioni normative o pronunciamenti dell'Autorità Garante per la protezione dei dati.

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) _____

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 :

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

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?

Allegato n. 2

DATA BREACH REPORT – USO INTERNO

Destinatari principali della segnalazione interna:

- Direttore Generale
- Responsabile della protezione dei dati
- Direttore Sanitario
- Direttore Amministrativo
- Responsabile dei Sistemi Informativi

STRUTTURA / UNITA' INTERESSATA	
RESPONSABILE STRUTTURA	
NOME E COGNOME DEL SEGNALANTE	
EMAIL	
TELEFONO	
BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI	
DETTAGLI TEMPORALI DELLA VIOLAZIONE (data, dal.. al , in corso)	
TIPOLOGIA DISPOSITIVO	□Computer □Rete □Dispositivo mobile □File o parte di un file □Strumento di backup □Documento cartaceo Altro: ……
TIPO 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: ……
DESCRIZIONE/UBICAZIONE DEI SISTEMI DI ELABORAZIONE E/O DI MEMORIZZAZIONE DEI DATI COINVOLTI	

QUANTI SOGGETTI SONO STATI COLPITI DALLA VIOLAZIONE DEI DATI	□N. persone …….. □Circa persone …… □Un numero (ancora) sconosciuto di persone
TIPOLOGIA DATI OGGETTO DI VIOLAZIONE	□Dati anagrafici/codice fiscale □Dati di accesso e di identificazione (username, password,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 genetici □Dati giudiziari □Copia per immagine su supporto informatico di documenti analogici □Ancora sconosciuto Altro:……
LIVELLO DI GRAVITA' DELLA VIOLAZIONE	□Basso/trascurabile □Medio □Alto □Molto alto
MISURE TECNICHE ED ORGANIZZATIVE APPLICATE AI DATI OGGETTO DI VIOLAZIONE	

Note:

……

……

……

……

……

……

……

……

……

……

……