



DELIBERAZIONE DEL DIRETTORE GENERALE
 D.G.R. n.891 del 29.10.2021 e D.P.G..R. n. 238 del 17.11.2021

N.

DEL / /

OGGETTO: Regolamento UE 201/679 (GDPR). Approvazione procedura per la gestione delle violazioni dei dati personali (Data Breach).

DESCRIZIONE	Data	Allegati n.
Documenti integranti il provvedimento		
Procedura Data Breach		1

U.O.S.D. PROPONENTE "URP - COMUNICAZIONE - UFFICIO STAMPA - PRIVACY"

Si attesta che la spesa di euro -----, relativa alla presente deliberazione costituisce:

- COSTO DI COMPETENZA DELL'ESERCIZIO
 INCREMENTO PATRIMONIALE

e che la spesa stessa rientra nelle previsioni di budget - conto economico

Il Dirigente dell'U.O.

U.O. Economico - Finanziaria

Si riscontra la corretta imputazione contabile della spesa proposta dall'U.O. di cui sopra.

- NON COMPORTA ONERI DI SPESA
 COMPORTA ONERI DI SPESA

Il Dirigente dell'U.O.
 Economico - Finanziaria

Il Direttore Generale, acquisito il parere favorevole di:

Direttore Amministrativo	
<input type="text"/>	<input type="text"/>

Direttore Sanitario	
<input type="text"/>	<input type="text"/>

IL DIRETTORE GENERALE

VISTI

il D.Lgs.30 dicembre 1992 n. 502 e successive integrazioni e modificazioni;

la Legge Regionale n 39/2001 smi;

l'articolo 2 comma 1 della legge regionale n. 12 del 1.7.2008 concernente la istituzione dal 1.1.2009 della Azienda Sanitaria Locale di Matera;

l'art. 2 della legge regionale n. 2 del 12.1.2017, relativo al "Nuovo assetto delle Aziende del Servizio Sanitario regionale";

RICHIAMATE

- la deliberazione n. 735 del 18.11.2021 concernente la presa d'atto del conferimento dell'incarico di Direttore Generale dell'Azienda Sanitaria Locale di Matera-ASM alla Dott.ssa Sabrina Pulvirenti;

- la deliberazione n. 736 del 18.11.2021 di conferimento dell'incarico di Direttore Sanitario dell'Azienda Sanitaria Locale di Matera al Dott. Giuseppe Magno;

- le deliberazioni n. 737 del 19.11.2021 di rettifica delle delibere 735 e 736 del 18.11.2021;

- la deliberazione n. 739 del 23-11-2021 di nomina di Direttore Amministrativo dell'Azienda Sanitaria di Matera ASM del dott. Massimiliano Gerli;

- la deliberazione n. 1135 del 19.12.2019 di conferimento al Dott. Achille Spada, dell'incarico triennale di Responsabile dell'U.O.S.D. "URP - Comunicazione - Ufficio Stampa - Privacy" a far data dal 01.01.2020;

VISTI

- il Regolamento Europeo 2016/679 (GDPR) relativo alla protezione delle persone fisiche e al trattamento dei dati personali, la cui entrata in vigore e piena applicazione ha determinato la necessità di declinare e implementare una governance aziendale puntuale in materia di protezione dei dati personali e di formalizzare precise scelte progettuali e di processo in una acclarata ottica di protezione dei dati fin dalla progettazione (privacy by design) e protezione dei dati per impostazione predefinita (privacy by default);
- il Decreto Legislativo 30 Giugno 2003 n. 196 "Codice in materia di protezione dei dati personali", come novellato dal D.Lgs 10 agosto 2018 n.101;

RILEVATO che:

- il Regolamento in oggetto è caratterizzato dalla centralità del "principio di responsabilizzazione" (c.d. accountability), e dalla introduzione nel nuovo quadro normativo di nuovi adempimenti, tra cui quelli previsti dagli artt. 33 e 34 del Regolamento UE e in particolare quello relativo all'adozione di una specifica procedura di gestione delle violazioni dei dati personali (Data Breach);
- ai sensi dell'art. 4, n. 12, del predetto Regolamento, per "violazione dei dati personali" si intende, "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";
- l'art. 33, paragrafo 1, del Regolamento suddetto prevede che "in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 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”;

- ai sensi dell'art. 34, paragrafo 1, del Regolamento suddetto “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”;

CONSIDERATO che:

- risulta necessario predisporre una procedura di gestione della violazione atta rilevare e limitare tempestivamente gli effetti di una violazione, valutare il rischio per i diritti e le libertà delle persone fisiche, stabilire se sia necessario notificare la violazione all'autorità di controllo e comunicarla alle persone fisiche interessate;
- la mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo potrebbe comportare l'imposizione di una sanzione al Titolare del trattamento ai sensi dell'art.83 del GDPR;
- la procedura per la gestione e notifica dei Data Breach disciplina il flusso degli adempimenti in caso di presunta o accertata violazione di dati personali degli incidenti di sicurezza, secondo le seguenti fasi:
 1. Predisposizione degli strumenti
 2. Rilevazione Evento - Acquisizione Notizia avvenuto incidente
 3. Analisi preliminare e invio segnalazione
 4. Gestione (contenimento del danno) e valutazione gravità dell'evento
 5. Notifica al Garante Privacy
 6. Altre segnalazioni dovute: (es. agli organi di Polizia e, nel caso di incidente informatico, a CERT-PA, all'autorità NIS competente)
 7. Comunicazione agli interessati, ove necessario, e raccolta riscontro dell'avvenuta comunicazione
 8. Inserimento dell'evento nel Registro delle Violazioni (Comprese le violazioni che non richiedono la notifica)
 9. Azioni correttive specifiche e per analogia

EVIDENZIATO che è stata predisposta, con il supporto di Liguria Digitale Spa, una procedura per la gestione e la notifica di data Breach in Azienda, allegata al presente atto per formarne parte integrante e sostanziale (Allegato 1);

RITENUTO di dover dare immediata esecutività al presente provvedimento al fine di consentire a questa Azienda di porre in essere tutte le azioni necessarie per assicurare la celere attivazione delle attività di che trattasi;

PRESO ATTO del parere del Direttore Amministrativo e del Direttore Sanitario, come innanzi espresso, con l'apposizione delle rispettive firme;

DELIBERA

- a) di approvare la “Procedura per la gestione delle violazioni dei dati personali. Data Breach (Artt.33 e 34 del Regolamento UE 2016/79)”, allegata al presente atto per formarne parte integrante e sostanziale (Allegato

1), che definisce il flusso degli adempimenti in caso di presunta o accertata violazione di dati personali degli incidenti di sicurezza, secondo le seguenti fasi:

1. Predisposizione strumenti
2. Rilevazione Evento - Acquisizione Notizia avvenuto incidente
3. Analisi preliminare e invio segnalazione
4. Gestione (contenimento del danno) e valutazione gravità dell'evento
5. Notifica al Garante Privacy
6. Altre segnalazioni dovute: (es. agli organi di Polizia e, nel caso di incidente informatico, a CERT-PA, all'autorità NIS competente)
7. Comunicazione agli interessati, ove necessario, e raccolta riscontro dell'avvenuta comunicazione
8. Inserimento dell'evento nel Registro delle Violazioni (Comprese le violazioni che non richiedono la notifica)
9. Azioni correttive specifiche e per analogia

b) di dare atto che la procedura approvata col presente provvedimento sarà soggetta ad aggiornamento anche in funzione di eventuali criticità riscontrate in sede di applicazione;

c) di programmare percorsi di formazione specifica, in materia di protezione e gestione delle violazioni dei dati personali;

d) di tramettere, a mezzo mail, all'indirizzo mail utenti@asmbsilicata.it, il presente provvedimento a tutti i dipendenti dell'Azienda individuati e nominati rispettivamente designati e autorizzati al Trattamento dei dati. La trasmissione all'indirizzo suddetto vale come notifica a tutti gli interessati.

e) di disporre la pubblicazione immediata dei dati contenuti nel presente atto sul sito aziendale - sezione "Amministrazione Trasparente" / Atti Generali, nonché nella sezione Privacy del sito aziendale;

f) di dichiarare il presente atto immediatamente eseguibile, attesa la necessità di assicurare la celere attivazione delle attività di che trattasi;

g) di dare atto che la documentazione richiamata nel presente provvedimento è agli atti dell'U.O. proponente.

Il Dirigente dell'U.O. dichiara, altresì, che la presente proposta deliberativa è conforme alle disposizioni di legge e regolamentari in materia.

L'Istruttore
Angela Divincenzo

Il Dirigente dell'U.O.
Achille Spada

Il presente verbale viene letto, approvato e sottoscritto.

Il Direttore Generale

CERTIFICATO DI PUBBLICAZIONE

Si certifica che, la presente Deliberazione è pubblicata all'Albo Pretorio Informatico dell'Azienda Sanitaria di Matera (ASM), sito web www.asmbasilicata.it, e che vi rimarrà per cinque giorni consecutivi. La relativa documentazione è disponibile per l'eventuale consultazione agli atti dell'U.O. proponente.

La stessa, ove non assoggettata al controllo regionale e ove non sia stata dichiarata immediatamente eseguibile, diventa esecutiva, ai sensi dell'art. 11, comma 11 e dell'art. 44 comma 8 della L.R. n. 39/2001, decorsi cinque giorni consecutivi dalla sua pubblicazione.

Trasmessa al Collegio Sindacale

Trasmessa alla Regione Basilicata - art. 44 comma 2 L.R. n. 39 del 31.10.2001

DEL / /

Il Responsabile

Il presente documento è un documento informatico originale in formato Pdf/A (conforme alle Regole tecniche pubblicato nel DPCM 22 febbraio 2013, previsti dall'art.71 del Codice dell' Amministrazione Digitale - D.lgs. n. 82/2005). Il documento è sottoscritto con firma digitale (verificabile con i software elencati sul sito dell' Agenzia per l' Italia Digitale) e/o con firma elettronica avanzata (firma grafometrica). In caso di stampa cartacea l'apposizione della firma digitale o comunque l'indicazione a stampa del soggetto firmatario rendono il documento cartaceo con piena validità legale ai sensi dell'art.4, comma 4 bis, del D.L. 18 ottobre 2012 n. 179.