

Sistema Socio Sanitario



Regione
Lombardia

ASST Ovest Milanese

DELIBERAZIONE N. 201 DEL 31/05/2018

OGGETTO

APPROVAZIONE DEL REGOLAMENTO AZIENDALE RELATIVO ALLA VIOLAZIONE DEI DATI PERSONALI - DATA BREACH (ARTT 33 E 34 DEL REG. UE 2016/679)

SU PROPOSTA DEL SERVIZIO AFFARI GENERALI E LEGALI

IL DIRIGENTE RESPONSABILE Laura Bonalumi

IL RESPONSABILE DEL PROCEDIMENTO Laura Bonalumi

Documento firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale e normativa connessa

IL DIRETTORE GENERALE

Visti gli artt 33 e 34 del Reg UE 2016/679 che disciplinano le modalità di notifica all'Autorità di controllo e di comunicazione all'interessato/i delle violazioni dei dati personali che possono verificarsi in ASST.

Ritenuto opportuno predisporre un Regolamento aziendale che fornisca indicazioni operative, calate nella realtà organizzativa dell'ASST Ovest Milanese, per la rilevazione dei cd. data breach (violazione dei dati personali).

Ritenuto altresì necessario definire dei criteri per valutare se la violazione dei dati rappresenti un rischio, o un rischio elevato, per i diritti e le libertà delle persone fisiche; condizioni poste dalla legge come necessarie per procedere rispettivamente con la notifica all'Autorità di controllo e con la comunicazione agli interessati.

Considerato che nell'ambito degli incontri organizzati da LIspa dall'inizio del 2018 ad oggi, sono state date informazioni ed è stato fornito materiale per l'elaborazione di criteri e metodi atti a valutare i casi di violazione.

Considerato quindi che la metodologia realizzata da ENISA (European Union Agency for Network and Information Security-working document, v1.0 december 2013) è stata proposta da LIspa come utile strumento per la valutazione dei casi di violazione delle banche dati elettroniche.

Ritenuto, in ogni caso, di avvalersi dei parametri contenuti nel Considerando 85 del REG UE 2016/679 anche per ipotesi di violazione non valutabili secondo il modello di cui sopra, secondo il parere condiviso nel "gruppo di valutazione" di cui al Regolamento aziendale oggetto di approvazione.

Ritenuto infatti necessario costituire un gruppo pluridisciplinare che supporti il Titolare nelle specifiche funzioni attribuite dal Regolamento UE, che viene qualificato nel regolamento aziendale come "gruppo di valutazione".

Sentito, per quanto di competenza, il parere favorevole del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio Sanitario;

DELIBERA

1. di approvare il Regolamento aziendale relativo alla violazione dei dati personali – Data Breach (artt 33 e 34 del Reg. UE 2016/679) allegato parte integrante e sostanziale del presente provvedimento.
2. di dare atto che l'esecuzione del presente provvedimento è affidata al Responsabile del procedimento il quale ne comunicherà l'avvenuta approvazione ai Servizi/Settori/UU.OO./Uffici interessati per l'adempimento delle rispettive competenze così come individuate nel P.O.A.;

3. di dare atto che, ai sensi dell'art. 17 - comma 6 - della L.R. 30 dicembre 2009 n° 33, così come introdotto dalla L.R. 23/2015, il presente provvedimento, non soggetto a controllo, è immediatamente esecutivo e verrà pubblicato all'Albo on-line sul sito informatico aziendale.

IL DIRETTORE GENERALE
(dott. Massimo Lombardo)