AZIENDA SANITARIA PROVINCIALE DI TRAPANI

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO

N.**20210000720** DEL **09/07/2021**

OGGETTO: **Adempimenti in applicazione del Regolamento UE 2016/79 (GDPR). Modifica procedura aziendale per la gestione delle violazioni dei dati personali (Data Breach). Provvedimento del 27/05/2021 del Garante per la Protezione dei Dati Personali.**

DIPARTIMENTO AMMINISTRATIVO SETTORE ECONOMICO FINANZIARIO E PATRIMONIALE	**PROPOSTA N. 20210000908 DEL 05/07/2021**
PROSPETTO DISPONIBILITA' **GESTIONE ANNO** **AUTORIZZAZIONE DI SPESA n.** **AUTORIZZAZIONE DI ENTRATA n.** CONTO: CONTO: CONTO: AUTORIZZAZIONE PRESENTE ATTO Euro	PROVENIENZA **Affari Generali Contratti e Convenzioni** U.O. **Contratti e Convenzioni** SEDE **Trapani** RESPONSABILE DEL PROCEDIMENTO **Dott.ssa Maria Scarpitta** RESPONSABILE U.O. **Dott.ssa Maria Scarpitta**

L'anno duemilaventuno, il giorno nove del mese di luglio presso la sede dell'Azienda Sanitaria Provinciale di Trapani, sita in Trapani nella via Mazzini n° 1

IL COMMISSARIO STRAORDINARIO

Dott. Paolo Zappalà, nominato con Decreto Assessoriale n. 695 del 31 Luglio 2020, acquisito il parere favorevole del Direttore Amministrativo Dott. Sergio Consagra e del Direttore Sanitario Dott.Gioacchino Oddo, ha adottato la seguente

DELIBERAZIONE

sottoscritta con firma digitale

OGGETTO: Adempimenti in applicazione del Regolamento UE 2016/79 (GDPR). Modifica procedura aziendale per la gestione delle violazioni dei dati personali (*Data Breach*). Provvedimento del 27/05/2021 del Garante per la Protezione dei Dati Personali.

IL RESPONSABILE U.O.C.
AFFARI GENERALI, CONTRATTI E CONVENZIONI
Dott.ssa Maria Scarpitta

VISTI il Regolamento Europeo 2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, la cui entrata in vigore ha implicato sia la necessità di definire in modo più preciso una *governance* aziendale in materia di protezione dei dati personali sia la necessità di attuare precise scelte progettuali e di processo in una acclarata ottica di "*privacy by design*" e "*privacy by default*";

il Decreto Legislativo 10 agosto 2018 n. 101 che ha integrato e modificato il Decreto Legislativo 30 Giugno 2003 n. 196 "Codice in materia di protezione dei dati personali";

RILEVATO che il Regolamento *de quo* prevede tra gli elementi caratterizzanti e innovativi il "principio di responsabilizzazione" (c.d. *accountability*), ponendo al centro del nuovo quadro normativo 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*);

che per "violazione dei dati personali" si intende, ai sensi dell'art. 4 comma 12, "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";

che l'art.33 del Regolamento suddetto recita: "nel 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";

che ai sensi dell'art.34 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";

che con Deliberazione del Commissario Straordinario n. 205 del 05/03/2021, l'Azienda approvava la "Procedura per la gestione delle violazioni dei dati personali *Data Breach (artt. 33 e 34 del Regolamento UE 2016/679)* adottando un Regolamento ad hoc allegato alla stessa;

CONSIDERATO che con Provvedimento del 27/05/2021 il Garante per la Protezione dei Dati Personali, ai sensi dell'art. 57, par. 1, lett. d), del Regolamento Europeo 2016/679 e dell'art. 37, comma 2, lett. b) del D. Lgs. N. 196/2003, ha inteso

modificare il contenuto e le modalità della notifica della violazione dei dati personali individuati nel Provvedimento n. 157 del 30/07/2019, adottando una procedura telematica disponibile nel portale dei servizio online dell'Autorità pubblicato all'indirizzo *https://servizi.gpdp.it/, attraverso la quale, a far data dal 1° luglio 2021, i titolari del trattamento forniscono al Garante le informazioni ivi richieste, ai sensi dell'art. 33 del Regolamento e dell'art. 26 del Decreto*;

che, pertanto, alla luce del citato provvedimento del 27/05/2021 del Garante per la Protezione dei Dati Personali, risulta variata la procedura di notifica della violazione dei dati personali individuati nel provvedimento n. 157 del 30/07/2019 e che, di conseguenza, va modificato il Regolamento allegato alla Deliberazione n. 205 del 05/03/2021 nella parte relativa alla "Notifica all'autorità di controllo", nel senso di seguito indicato:

Il testo dell'art. 6.4 del Regolamento "Notifica all'autorità di controllo" sarà sostituito dal seguente:

"Art. 6.4 Notifica all'autorità di controllo. Ai sensi dell'art. 33 del GDPR, la notifica del Data Breach all'Autorità di controllo è sempre obbligatoria, salvo i casi in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Pertanto, rilevata l'esistenza di un rischio per i diritti e le libertà degli interessati e ritenuto doversi effettuare la notifica della violazione dei dati subita, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Azienda dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza, utilizzando la procedura telematica disponibile nel portale dell'Autorità pubblicato all'indirizzo https://servizi.gpdp.it/. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, essa dovrà essere corredata dei motivi del ritardo.
Se non fosse possibile fornire tutte le informazioni contestualmente, queste ultime potranno essere inviate in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non sono disponibili.
In questo caso sarà cura del Titolare del trattamento raccogliere le informazioni mancanti e procedere, senza ritardo, alle integrazioni eventualmente necessarie avvalendosi della collaborazione delle strutture interessate che, a tal fine, dovranno prestare pronta, piena e fattiva disponibilità.
La mancata collaborazione del personale e strutture coinvolte assume rilevanza ai fini disciplinari e contrattuali.
Ai sensi dell'art. 33 del GDPR, la notifica all'autorità di controllo deve contenere almeno i seguenti contenuti:
"a) descrizione della 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) indicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrizione delle probabili conseguenze della violazione dei dati personali;
d) descrizione delle 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".
La violazione sarà effettuata dal titolare del trattamento tramite PEC con indicazione del D.P.O. come punto di contatto con l'Autorità di controllo";

RITENUTO che deve essere data 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;

DATO ATTO che il Responsabile della Struttura che propone il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata, è conforme alla normativa vigente con riferimento alla materia trattata ed è, sia nella forma che nella sostanza, totalmente legittimo, veritiero ed utile per il servizio pubblico, ai sensi e per gli effetti di quanto disposto dall'art. 1 della L. 14 gennaio 1994 n. 20 e s.m.i., e che lo stesso è stato predisposto nel rispetto della L. 6 novembre 2012 n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione", nonché nell'osservanza dei contenuti del vigente Piano Aziendale della Prevenzione della Corruzione, con particolare riferimento all'assenza di situazioni di conflitto d'interesse in relazione all'oggetto dell'atto e alla tematica connessa.

PROPONE

Per le causali di cui in premessa:

1) **Approvare** la "Procedura per la gestione delle violazioni dei dati personali. *Data Breach* (Artt.33 e 34 del Regolamento UE 2016/79)" con le modifiche apportate dal Provvedimento n. 157 del 30/07/2019 del Garante per la Protezione dei Dati Personali, così come da documento allegato alla presente – modificato come sopra indicato -, che ne fa parte integrante, che comprende il flusso degli adempimenti in caso di presunta o accertata violazione di dati personali degli incidenti di sicurezza, secondo le seguenti fasi:

   - Rilevazione e segnalazione del *Data Breach*;
   - Identificazione, analisi e valutazione del *Data Breach*;
   - Valutazione del rischio per i diritti e le libertà delle persone fisiche;
   - Notifica all'autorità di controllo;
   - Comunicazione all'interessato;
   - Registrazione del *Data Breach*;

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

3) **Notificare** il presente provvedimento a tutte le strutture aziendali tramite la pubblicazione sul sito *web* aziendale, Sezione Privacy;

4) **Trametterе** il presente provvedimento al Gruppo di Lavoro *Privacy*, costituito giusta Delibera n. 3074 del 22/11/2019;

5) **Incaricare** Il D.P.O. aziendale e l'Ufficio Protezione dei dati personali dell'esecuzione del presente provvedimento.

L'ESTENSORE DEL PROVVEDIMENTO
(*Dott. Giancarlo Provenzano*)

IL RESPONSABILE DEL PROCEDIMENTO
(*Dott.ssa Maria Scarpitta*)

IL RESPONSABILE DELLA STRUTTURA PROPONENTE
(*Dott.ssa Maria Scarpitta*)

IL COMMISSARIO STRAORDINARIO

VISTA la proposta di deliberazione che precede e che si intende qui di seguito integralmente riportata e trascritta;

RITENUTO di condividerne il contenuto;

DELIBERA

di adottare la proposta di deliberazione per come sopra formulata dal Dirigente Responsabile della Struttura proponente e, conseguentemente:

1) **Approvare** la "Procedura per la gestione delle violazioni dei dati personali. *Data Breach* (Artt.33 e 34 del Regolamento UE 2016/79)" con le modifiche apportate dal Provvedimento n. 157 del 30/07/2019 del Garante per la Protezione dei Dati Personali, così come da documento allegato alla presente – modificato come sopra indicato -, che ne fa parte integrante, che comprende il flusso degli adempimenti in caso di presunta o accertata violazione di dati personali degli incidenti di sicurezza, secondo le seguenti fasi:

   - Acquisizione di notizia di *Data Breach*;
   - Identificazione dell'evento e sua valutazione;
   - Valutazione del rischio per i diritti e le libertà delle persone fisiche;
   - Notifica all'autorità di controllo;
   - Comunicazione all'interessato;
   - Registrazione del *Data Breach*;

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

3) **Notificare** il presente provvedimento a tutte le strutture aziendali tramite la pubblicazione sul sito *web* aziendale, Sezione Privacy;

4) **Trametterе** il presente provvedimento al Gruppo di Lavoro *Privacy*, costituito giusta

Delibera n. 3074 del 22/11/2019;

5) **Incaricare** Il D.P.O. aziendale e l'Ufficio Protezione dei dati personali dell'esecuzione del presente provvedimento.

La presente deliberazione è composta – escluso il frontespizio – da n. 5 pagine ed è firmata digitalmente.