Delibera 23-2023: Approvazione procedura per la gestione di data breach ai sensi del regolamento (ue) n. 679/2016

IL CONSIGLIO DI AMMINISTRAZIONE

VISTA la Legge Regionale n. 17 del 24/06//2011 avente ad oggetto "*Riordino delle Istituzioni Pubbliche di Assistenza e Beneficenza (IPAB) e disciplina delle Aziende Pubbliche di Servizi alla Persona (ASP)*";

PREMESSO che con Delibera di Giunta Regionale n. 109 del 24/02/2014 avente ad oggetto "*L.R. 24/06/2011, nr. 17, come modificata ai sensi dell'art. 1, comma 1 , L.R., 25.11.2013, nr. 43 – Costituzione dell'Azienda Pubblica di Servizi alla Persona- ASP N. 2 della Provincia di Teramo – Determinazione numerica dei membri dell'Assemblea dei soggetti portatori di interesse, L.R. nr. 17/2011, art. 9.*" è stata costituita l'Azienda Pubblica di Servizi alla Persona - A.S.P. n. 2 della Provincia di Teramo, mediante trasformazione in Azienda Pubblica di 4 ex IPAB insistenti sul territorio intraprovinciale aventi i requisiti previsti per la trasformazione, tra le quali l'IPAB Istituto Castorani di Giulianova (TE);

VISTO lo Statuto dell'ASP, omologato ai sensi dell'art. 8, comma 4 della Legge Regionale n. 17 del 24/06//2011 con Delibera di Giunta Regionale n. 367 del 15/05/2015;

VISTO il D.Lgs. 267/2000;

VISTA la Legge n. 328/2000 art. 1 comma 3 – legge quadro per la realizzazione del sistema integrato di interventi e servizi sociali che attribuisce la programmazione e l'organizzazione agli enti locali, alle Regioni ed allo Stato ai sensi del D.Lgs n. 112 del 31.03.1998;

RILEVATO CHE la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale é un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

CONSIDERATO CHE le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:

- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

TENUTO PRESENTE CHE tale evoluzione ha indotto l'Unione europea ad adottare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

DATO ATTO CHE il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

VISTO il D.lgs 196/2003, modificato dal D.Lgs. 10 agosto 2018 n. 101;

DATO ATTO CHE il GDPR introduce l'obbligo di notificare all'autorità di controllo nazionale (Garante Privacy) incidenti sulla sicurezza che comportino la violazione dei dati personali (data breach) e di rendere nota la violazione stessa alle persone fisiche interessate;

DATO ATTO CHE la notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- descrizione della natura della violazione dei dati personali e le registrazioni dei dati personali in questione;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o da adottare 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.

TENUTO PRESENTE CHE la violazione dei dati personali è da intendersi come 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 tale da impedire al titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR.;

DATO ATTO CHE, 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, e che tale comunicazione deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali, contenendo obbligatoriamente i seguenti contenuti minimi:

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

RILEVATO CHE, per quanto sopra, è necessario istituire:
1. una Procedura data breach
2. un registro interno data breach, dove vengono annotate sia le violazioni non notificabili che quelle notificabili, il quale deve contenere i seguenti dati:

- i dettagli relativi alla violazione (cause, fatti e dati personali interessati);
- gli effetti e le conseguenze della violazione;
- i provvedimenti adottati per porvi rimedio;
- il ragionamento alla base delle decisioni prese in risposta a una violazione (con particolare riferimento alle violazioni non notificate ed alle violazioni notificate con ritardo);

DATO ATTO CHE la Procedura data breach, avente lo scopo di indicare le modalità di gestione del data breach, garantisce la realizzabilità tecnica e la sostenibilità organizzativa;

DATO ATTO CHE, al fine di garantire la massima diffusione interna ed esterna e la massima conoscibilità sulle azioni da intraprendere e sui comportamenti da adottare in caso di data breach, è disposta la pubblicazione della Procedura data breach sul sito web istituzionale nella sezione "Amministrazione Trasparente", sottosezione di primo livello "Altri Contenuti", sottosezione di secondo livello "Privacy", nonché a garantire la conoscibilità della stessa a tutti i dipendenti dell'Ente;

VISTI:

- D.Lgs. 267/2000;
- Legge 241/1990;
- D.Lgs. 196/2003;
- Legge 190/2012;
- D.Lgs. 33/2013;
- Regolamento (UE) n. 679/2016;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee Guida EDPB del 02 marzo 2021 con esempi riguardanti la notificazione del data breach;
- Provvedimento del Garante della protezione dei dati personali del 27 maggio 2021;

VISTO il parere di regolarità tecnica;

Con voti unanimi, resi nei modi di legge dai Consiglieri presenti e votanti

D E L I B E R A

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

1. di approvare la procedura per la gestione di data breach ai sensi del regolamento (ue) n.679/2016, allegata alla presente, per formarne parte integrante e sostanziale;

2. di disporre che al presente provvedimento venga assicurata:
   a) la pubblicità legale con pubblicazione all'albo pretorio
      nonché
   b) la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "amministrazione trasparente", sezione di primo livello "disposizioni generali" sezione di secondo livello "atti generali";

3. di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal gdpr n. 2016/679;

4. di dare atto che ai fini della pubblicità e trasparenza amministrativa il presente atto sarà pubblicato all'albo pretorio on line per 15 giorni secondo quanto previsto dalle disposizioni vigenti.

Con separata votazione

DELIBERA

di dichiarare il presente atto immediatamente esecutivo.

Il Segretario verbalizzante della seduta
Dott.ssa Alessandra Troiani
Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 del D.L. 39/93

Visto: si esprime parere favorevole in merito alla regolarità contabile del presente atto
Il Responsabile del Servizio
Dott.ssa Alessandra Troiani
Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 del D.L. 39/93

Visto: si esprime parere favorevole in merito alla regolarità tecnica del presente atto
Il Direttore
Dr. Gabriele Astolfi
Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 del D.L. 39/93

Avv. Giulia Palestini Presidente
Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 del D.L. 39/93

Sig. Antonio Samuele Componente
Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 del D.L. 39/93

AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA

ASP N. 2 DELLA PROVINCIA DI TERAMO

SEDE LEGALE

Via Pietro Baiocchi, n. 29 – ATRI (Te)

VERBALE DI DELIBERAZIONE

N. 23 del 02/08/2023

OGGETTO

Approvazione procedura per la gestione di data breach ai sensi del regolamento (ue) n. 679/2016

Il giorno 02 agosto 2023 alle ore 12:00 presso la Sede Legale della Asp. N. 2 della Provincia di Teramo, si è riunito il Consiglio di Amministrazione, composto dalle seguenti persone:

1) Avv. Giulia Palestini Presidente
2) Sig. Antonio Samuele Componente
3) --------

Funge da Segretario del CDA la dott.ssa Alessandra Troiani, Responsabile Area Amministrativa e Finanziaria dell'Asp 2 Teramo di Atri (Te)

CERTIFICATO DI PUBBLICAZIONE

Il sottoscritto Direttore certifica che la presente deliberazione viene pubblicata all'Albo Pretorio dell'Ente per 15 giorni consecutivi, a far data dal

Il Direttore
Dr. Gabriele Astolfi
Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 del D.L. 39/93