COMUNE DI ALBA ADRIATICA
PROVINCIA DI TERAMO

DELIBERAZIONE DELLA GIUNTA COMUNALE

Numero 8 Del 09-02-22

COPIA

Oggetto: APPROVAZIONE PROCEDURA PER LA GESTIONE DI DATA BREACH AI SENSI DEL REGOLAMENTO (UE) N.679/2016 .

L'anno duemilaventidue il giorno nove del mese di febbraio alle ore 13:00, presso questa Sede Municipale, convocata nei modi di legge, si è riunita la Giunta Comunale per deliberare sulle proposte contenute nell'ordine del giorno unito all'avviso di convocazione.

Dei Signori componenti della Giunta Comunale di questo Comune:

Casciotti Antonietta	**Sindaco**	**P**
Ciccarelli Alessandra	**Assessore**	**P**
Pulcini Simone	**Assessore**	**P**
Di Matteo Francesca	**Assessore**	**P**
Cichetti Paolo	**Assessore**	**P**
Colonnelli Nicolino	**Assessore esterno**	**P**

ne risultano presenti n. 6 e assenti n. 0.

Assume la presidenza il Signor Casciotti Antonietta in qualità di Sindaco assistito dal SEGRETARIO COMUNALE Dott.ssa Piro Emilia.

Il Presidente, accertato il numero legale, dichiara aperta la seduta ed invita la Giunta Comunale ad esaminare e ad assumere le proprie determinazioni sulla proposta di deliberazione indicata in oggetto.

Visti:
- la legge 7 agosto 1990, n. 241 e successive modificazioni e integrazioni;
- il D.Lgs. 18 agosto 2000, n. 267, "Testo Unico delle leggi sull'ordinamento degli Enti Locali";
- il Regolamento di Organizzazione degli Uffici e dei Servizi;
- lo Statuto ed il Regolamento di Contabilità dell'Ente;
- i pareri resi, a norma dell'art. 49 del D.Lgs. 267/2000, dal Responsabile dell'Area e/o Ufficio interessato e dal Responsabile dell'Area Economia e Finanza in ordine, rispettivamente, alla regolarità tecnica e contabile sulla proposta della presente deliberazione;

La presente seduta della Giunta Comunale viene svolta in presenza, adottando le misure preventive di carattere igienico - sanitario precauzionali di cui al D.P.C.M. dell'8 marzo 2020 art. 1 lett.q) e successive disposizioni, quali frequente areazione del locale e adeguata distanza, assicurando quindi il rispetto della distanza interpersonale di un metro (cd. *distanza droplet*).
Si dà atto altresì del rispetto delle indicazioni riportate nel DPCM del 18/10/2020 e della circolare del Ministero dell'Interno prot. n. 14553 del 27/10/2020

LA GIUNTA COMUNALE

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 la Procedura data breach verrà pubblicata 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;

Visti i pareri resi, a norma dell'art. 49 del D.Lgs. 267/2000, che si riportano integralmente nel presente atto:

PARERE: Favorevole in ordine alla **REGOLARITA' TECNICA**
Data: 07-02-2022 Il Responsabile del servizio

ZARROLI ERMINIA

AD UNANIMITA' di voti favorevoli legalmente espressi,

DELIBERA

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 TRASMETTERE copia del presente provvedimento al GDPR.

Infine la Giunta Comunale, stante l'urgenza di provvedere, con voti unanimi.

DELIBERA

di dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'articolo 134, comma 4, del d.Lgs. n. 267/2000

PROCEDURA GESTIONE DATA BREACH

1. Che cos'è il Data Breach

Il *data breach* consiste nella violazione dei dati personali gestiti da una organizzazione 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.

Il Regolamento UE sulla protezione dei dati personali, GDPR n. 2016/679, disciplina il *data breach* prevedendo espressamente un obbligo di notifica e comunicazione in capo al titolare del trattamento in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati, quali quelli relativi ai dati sensibili e giudiziari previsti dall'art. 9 del GDPR.

2. Rilevazione identificazione e classificazione degli eventi

La fase di rilevazione, identificazione e classificazione dell'evento è particolarmente critica in quanto comporta o il riconoscimento dell'incidente, e quindi la sua gestione, oppure l'archiviazione dell'evento.

Relativamente alla rilevazione dell'evento, la segnalazione di un evento potenzialmente identificabile come incidente può provenire da diverse fonti, quali:

- personale interno;
- terze parti;
- sistemi di monitoraggio della sicurezza fisica o logica.

Le segnalazioni possono provenire dal servizio di Help Desk, dai sistemisti o dagli utenti stessi. Tutte queste segnalazioni indirizzate vengono analizzate e classificate.

Una volta che l'incidente è identificato e classificato, vengono determinate le seguenti variabili:

- l'urgenza dell'intervento;
- l'impatto dell'evento sull'operatività dell'Amministrazione (es. importanza del servizio impattato);
- nel caso l'evento non presenti conseguenze, esso deve essere comunque tracciato;
- nel caso l'evento venga classificato come incidente di sicurezza deve essere comunicato al Titolare del trattamento, al DPO-RPD Responsabile della protezione dei Dati, al Responsabile del servizio, al CED ove esistente, al fine di avviare la fase di gestione.

Successivamente all'identificazione e classificazione dell'evento, il Titolare del trattamento, nel caso l'evento venga classificato come incidente di sicurezza, può prevedere la creazione di un IRT (Incident Response Team) al fine di avviare la fase di gestione.

Nel caso in cui non sia creato l'IRT, il Titolare del trattamento, sentito il DPO, dà disposizioni affinché si provveda alla registrazione dell'evento, secondo opportune modalità, in funzione della tipologia di evento segnalato.

dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

5. Descrizione del flusso

Il flusso di comunicazione al Garante da parte dell'Ente prevede i seguenti passi:

1. Il Titolare del trattamento o l'IRT, se nominato, nel corso della gestione di un incidente di sicurezza informatica, riscontra una compromissione di dati personali (Data Breach).
2. Gli uffici impattati, valutano l'effettiva perdita o diffusione di dati personali e le informazioni contenute nel modulo compilato.
3. In caso di valutazione con rilevamento di violazione dei dati personali, che presenti un probabile rischio per i diritti e le libertà delle persone fisiche, gli uffici impattati informano il Titolare del trattamento o l'IRT, se nominato, inviando le informazioni raccolte.
4. il Titolare del trattamento o l'IRT, se nominato, di concerto con il DPO/RPPD Responsabile della protezione dei dati, valutano il livello di gravità della violazione in funzione della significatività dell'impatto della violazione avvenuta sui dati personali contenuti nelle banche dati di propria titolarità eseguendo un'autovalutazione attraverso il tool messo a disposizione sul sito web del Garante della protezione dei dati personali accessibile dal seguente link: https://servizi.gpdp.it/databreach/s/self-assessment .

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

Questo strumento, a disposizione di ciascun titolare del trattamento di dati personali, consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Mediante alcuni semplici quesiti, il titolare viene guidato nell'assolvimento degli obblighi in materia di **«Notifica di una violazione dei dati personali all'autorità di controllo»** (art. 33Apertura sito esterno in una nuova scheda per l'articolo 33 del Regolamento (UE) 2016/679 del Regolamento (UE) 2016/679 o art. 26 del D.Lgs. 51/2018) e di **«Comunicazione di una violazione dei dati personali all'interessato»** (art. 34Apertura sito esterno in una nuova scheda per l'articolo 34 del Regolamento (UE) 2016/679 del Regolamento (UE) 2016/679 o art. 27 del D.Lgs. 51/2018). Questo strumento è da considerarsi esclusivamente quale ausilio al processo decisionale del titolare del trattamento e non rappresenta il pronunciamento dell'Autorità sull'applicazione del Regolamento (UE) 2016/679 o del D.Lgs. 51/2018. Le informazioni fornite durante il suo utilizzo non saranno conservate.

Nel caso in cui la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 33 del GDPR, la notifica all'autorità di controllo deve essere effettuata entro 72 ore, diminuite a 48 ore per gli Enti della Pubblica Amministrazione secondo quanto previsto dal Provvedimento del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach).

Qualora la notifica all'autorità di controllo sia effettuata oltre i termini previsti, è corredata dei motivi del ritardo.

dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda.

La presente procedura sarà oggetto di periodiche revisioni e adeguamenti in relazione alle norme di armonizzazione che saranno emanate, a variazioni nelle misure di sicurezza da adottare e conseguenti modifiche procedurali.

8. Chiusura degli incidenti

A seguito dell'implementazione delle contromisure e della valutazione della loro efficacia, l'Ente/Azienda dichiara l'incidente chiuso in modo formale, verificando che siano state prodotte dall'IRT, se nominato, le seguenti evidenze:

- l'analisi relativa alle modalità di gestione dell'evento al fine di valutare i tempi di risposta, la metodologia utilizzata, ecc. ed al fine di verificare la necessità di modifiche od integrazioni nella procedura e/o policy in essere;
- la stesura di un rapporto relativo all'incidente di sicurezza, da condividere con i dirigenti responsabili delle strutture coinvolte, in modo da riportare le problematiche di sicurezza verificatesi e tenerne traccia.
  Il rapporto deve essere consegnato tempestivamente e deve contenere, necessariamente, i seguenti punti:
  - descrizione dell'evento, dalla sua segnalazione al ripristino dell'operatività;
  - esposizione di tutte le prove raccolte e di tutte le ricerche effettuate con i relativi risultati;
  - ipotesi sulle cause dell'incidente;
  - proposte di miglioramento e azioni correttive;
  - l'esecuzione delle azioni correttive proposte ed approvate.

A conclusione dell'incidente l'IRT (Incident Response Team), se nominato, deve trasmettere una dettagliata relazione al Titolare del Trattamento.

Data _____

Il Titolare del trattamento

PROPOSTA DI DELIBERAZIONE DELLA GIUNTA COMUNALE
N. 21 DEL 07/02/2022

DELIBERAZIONE DELLA GIUNTA COMUNALE
N. 8 DEL 09-02-2022

Art. n. 49 del D.LGS. 18.08.2000, n. 267

Art. N. 49 del D.Lgs. 18.08.2000, n. 267, come sostituito dall'art. 3, comma 1, lett. b) della Legge 213/2012.

ATTESO il rispetto delle prescrizioni contenute nel documento di conformità, come adottato dal Segretario Comunale con proprio atto n. 1 del 20/02/2019 e comunicato agli uffici con nota circolare n.5650 del 22/02/2019".

In ordine alla **regolarità TECNICA** si esprime parere FAVOREVOLE per quanto di competenza

Il Responsabile del Servizio
Dott.ssa Erminia Zarroli

Alba Adriatica, lì 07/02/2022

ATTESO il rispetto delle prescrizioni contenute nel documento di conformità, come adottato dal Segretario Comunale con proprio atto n. 1 del 20/02/2019 e comunicato agli uffici con nota circolare n.5650 del 22/02/2019".

In ordine alla regolarità CONTABILE si esprime parere _____

☐ comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente.

☒ non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente.

Alba Adriatica, lì 09 FEB 2022

Il Responsabile
Ufficio Bilancio e Organizzazione
Dott.ssa Loredana Cimini

Il presente verbale viene letto, approvato e sottoscritto.

Il Sindaco	Il Segretario Generale
F.to Prof.ssa Casciotti Antonietta	F.to Piro Emilia

La presente Deliberazione:

- viene pubblicata, in data odierna e per 15 giorni consecutivi, sul sito web istituzionale di questo Comune accessibile al pubblico *(art. 32, comma 1, della legge 18 giugno 2009, n. 69)* ed è stata compresa, in data odierna, nell'elenco, delle deliberazioni comunicate ai capigruppo consiliari *(art. 125, del T.U. n. 267/2000).*

(_X_) - diventa esecutiva in data odierna, ai sensi dell'art. 134, comma 4, del D.Lgs. 18.08.2000, n. 267.

(___) – diventa esecutiva decorso il termine di giorni dieci dalla sua pubblicazione ai sensi dell'art. 134, comma 3 del D.Lgs.18.08.2000, n. 267.

Alba Adriatica, lì 09/02/2022

IL SEGRETARIO GENERALE
F.to Piro Emilia

Copia conforme all'originale per uso amministrativo.

Alba Adriatica, lì 09/02/2022

IL SEGRETARIO GENERALE
Dott.ssa Piro Emilia