COMUNE DI VERRUA PO

PROVINCIA DI PAVIA

Codice Ente 11312

N. 55 Reg. Delib. del 08/11/2021

ORIGINALE

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

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

L'anno **duemilaventuno**, addì **otto** del mese di **novembre**, alle ore **dodici** e minuti **trenta**, nella sede comunale si è riunita la GIUNTA COMUNALE.

All'appello risultano:

Cognome e Nome	Carica	Presente
LAZZARI PIERANGELO	*Sindaco*	Sì
MONTIS CLAUDIA	*Vice Sindaco*	Sì
BELLIERO MARCO	*Assessore*	Sì

Totale PRESENTI	3
Totale ASSENTI	0

Assiste il ViceSegretario Comunale Sig. Dott. Umberto FAZIA MERCADANTE il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti Il Sig LAZZARI PIERANGELO, assume la Presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

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

LA GIUNTA COMUNALE

Richiamata la delibera di CC n. 16 del 29.04.2019 avente ad oggetto: *"Esame ed approvazione regolamento comunale di attuazione del regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali";*

Rilevato che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo "GDPR");

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;
Rilevato che, con il GDPR, è stato richiesto agli Stati membri un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;
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 renderenota 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 inquestione;*
- *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 contenutiminimi:

- 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 ad 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;

– il responsabile del procedimento, è il Segretario Comunale e che lo stesso, 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 tenuto a garantire 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;

– il procedimento di adozione e approvazione della Procedura *Data Breach* e del registro *Data Breach* e il presente provvedimento, risultano mappati dal PTPC e che sono stati effettuati i controlli previsti dal Regolamento Sistema controlli interni ed è stato rispettato quanto previsto dal Piano Triennale di Prevenzione della corruzione e dal Programma per la trasparenza;

CONSIDERATO che con delibera di Giunta Unione n° 4 del 20.02.2020 è stato affidato l'incarico di responsabile della Protezione dati (DPO) all'Avvocato stab. Erika Bianchi nata a Pavia il 15 aprile 1985, C.F. BNCRKE85D55G388A, per le annualità 2020 e 2022 per l'Unione dei Comuni e per i Comuni di Verrua Po e Rea;

Visti:

- D.Lgs. 267/2000;
- Legge 241/1990;
- D.Lgs. 196/2003;
- Legge 190/2012;
- D.Lgs. 33/2013;
- Regolamento Generale sulla protezione dei dati personali (UE) 2016/679
- Decreto Legislativo n. 196/2003, come novellato dal D.Lgs. n. 101/2018
- Regolamento per l'attuazione del Regolamento UE 2016/679 relativo alla protezione e trattamento dei dati personali.
- Linee guida WP art. 29.

Visto il parere favorevole espresso dal Responsabile del Servizio in ordine alla regolarità tecnica delpresente atto (art. 49, 1 comma, D.Lgs. 267/2000);

Con voti unanimi e favorevoli resi in forma palese.

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 la pubblicità legale con pubblicazioneall'Albo Pretorio nonché la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "AmministrazioneTrasparente", sezione di primo livello "Disposizioni generali" sezione di secondo livello "Atti generali";
3. DI DARE ATTO che, in disparte la pubblicazione sopra indicata, chiunque ha diritto, ai sensi dell'art. 5 comma 2 D.Lgs. 33/2013 di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del citato D.Lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto.
4. DI DISPORRE che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal D.Lgs. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.
5. DI DICHIARARE, con separata ed unanime votazione, il presente provvedimento immediatamente eseguibile ai sensi dell'articolo 134, comma 4, del decreto legislativo 18 agosto 2000, n. 267, in ragione dell'esigenza di celerità correlate dei procedimenti amministrativi.

Fatto, letto e firmato.

IL PRESIDENTE
f.to LAZZARI PIERANGELO

IL VICESEGRETARIO COMUNALE
f.to Dott. Umberto FAZIA MERCADANTE

CERTIFICATO DI PUBBLICAZIONE

Il sottoscritto attesta che la presente deliberazione viene pubblicata in data odierna, per rimanervi per 15 gg. consecutivi ai sensi dell'art. 124, comma 1, del D.Lgs. n. 267/2000 e s.m.i. all'Albo Pretorio Informatico di questo Comune (art. 32, comma 1, della Legge 18/06/2009, n. 69).

Verrua Po, lì _____

IL RESPONSABILE DELLE PUBBLICAZIONI
f.to Carmen ROVATI

COMUNICAZIONE AI CAPIGRUPPO

Nello stesso giorno in cui è stato affisso all'Albo Pretorio, il presente verbale viene trasmesso in elenco ai Capigruppo Consiliari ai sensi dell'art. 125 del Decreto Legislativo 267/2000 e s.m.i.

Verrua Po, lì _____

IL VICESEGRETARIO COMUNALE
f.to Dott. Umberto FAZIA MERCADANTE

Copia conforme all'originale, in carta libera per uso amministrativo.

Verrua Po, lì _____

IL VICESEGRETARIO COMUNALE
(Dott. Umberto Fazia Mercadante)

_____

CERTIFICATO DI ESECUTIVITA'

- ☐ Perché dichiarata immediatamente eseguibile (art. 134, 4° comma, D.Lgs. 18 agosto 2000, n. 267)
- ☐ Per la scadenza dei 10 giorni della pubblicazione (art. 134, 3° comma, D.Lgs. 18 agosto 2000, n. 267)

Verrua Po, lì _____

IL VICESEGRETARIO COMUNALE
Dott. Umberto Fazia Mercadante