COMUNE DI CAPPELLA CANTONE
(Prov. di Cremona)

Originale

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N. 54 del 06/10/2022

OGGETTO: **Approvazione procedura di gestione delle violazioni dei dati personali**

L'anno **duemilaventidue,** addì **sei** del mese di **Ottobre** alle ore **12,00** nella sala della adunanze.
Previa l'osservanza di tutte le formalità prescritte dalla vigente legge, vennero oggi convocati a seduta i componenti la Giunta Comunale.

All'appello risultano:

MONFREDINI Francesco	Sindaco	SI
TADI Pierluigi	Assessore	SI
BETTONI Simona Iside	Assessore	SI
PRESENTI: **3**	ASSENTI**:0**	

Partecipa all'adunanza il Vice Segretario Comunale Sig. **Dr. Alfredo Zanara**, il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti, il Sig. **Monfredini Francesco** nella sua qualità di Sindaco assume la presidenza e dichiara aperta la seduta per la trattazione dell'argomento indicato in oggetto.

G.C. n. 54 del 06/10/2022
Oggetto: **Approvazione procedura di gestione delle violazioni dei dati personali**

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, 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 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 il responsabile del procedimento, è il Segretari Generale 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;

Dato atto che 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;

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;
Parere del WP29 sulla limitazione della finalità - 13/EN WP
203;
Statuto Comunale;
Regolamento di organizzazione degli uffici e dei Servizi;
Regolamento sul trattamento dei dati sensibili;
Codice di comportamento interno
dell'Ente; Circolari e direttive del RPC;

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

con voti unanimi favorevoli,

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 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.

Con separata votazione,

Delibera

Di dichiarare la presente deliberazione immediatamente esecutiva

IL SINDACO
Francesco Monfredini

Il Vice Segretario Comunale
Dott. Alfredo Zanara

RELATA DI PUBBLICAZIONE

SI CERTIFICA CHE COPIA DELLA PRESENTE E' STATA AFFISSA ALL'ALBO PRETORIO DEL COMUNE IN DATA ODIERNA E VI RIMARRA' PER 15 GIORNI CONSECUTIVI.

Cappella Cantone lì, _____

Il Vice Segretario Comunale
Alfredo Zanara

ESECUTIVITA' DELLA

DELIBERAZIONE Il sottoscritto Segretario Comunale,

ATTESTA

Che la presente Deliberazione è divenuta esecutiva per:

Decorrenza giorni 10 dall'inizio della pubblicazione (art. 34, comma 3, del D.Lgs. 18/08/2000, n° 267)

Dichiarazione di immediata eseguibilità (art. 134, comma 4, del D.Lgs. 18/08/2000, n° 267;

Lì, 06/10/2022

Il Vice Segretario Comunale
Dott. Alfredo Zanara

Per copia conforme all'originale;

Lì, 06/10/2022

Il Vice Segretario Comunale
Dott. Alfredo Zanara

_____