COMUNE DI CANEGRATE PROVINCIA DI MILANO CODICE 10934	NUMERO 164	DATA 25-11-2020

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

COPIA

DELIBERAZIONE DELLA GIUNTA COMUNALE

SI DÀ ATTO CHE, AI SENSI DELL'ART. 73 DL 17/03/2020 N. 18 E SUCCESSIVI, E DEL DECRETO SINDACALE N. 5 DEL 23/03/2020, LA SEDUTA DI GIUNTA COMUNALE SI È TENUTA IN MODALITÀ VIDEOCONFERENZA TRAMITE PIATTAFORMA GOTOMEETING, IL GIORNO **25/11/2020** ALLE ORE **18.00.**

ALL'APPELLO RISULTANO:

COMPONENTE	P.	A.G.	A.I.	COMPONENTE	P.	A.G.	A.I.
COLOMBO ROBERTO	X			MERAVIGLIA FRANCA	X		
MODICA MATTEO	X			SPIRITO DAVIDE	X		
AUTERI GIUSEPPINA	X			ZAMBON EDOARDO	X		

TOTALE PRESENTI 6 TOTALE ASSENTI 0

ASSISTE IL SEGRETARIO GENERALE DOTT.SSA TERESA LA SCALA

ESSENDO LEGALE IL NUMERO DEGLI INTERVENUTI, IL SINDACO ROBERTO COLOMBO ASSUME LA PRESIDENZA E DICHIARA APERTA LA SEDUTA, PER LA TRATTAZIONE DELL'OGGETTO SOPRA INDICATO.

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

LA GIUNTA COMUNALE

Premesso

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 Regolamento o "GDPR").

Rilevato che il GDPR è diventato definitivamente applicabile in via diretta in ciascuno degli Stati membri dell'Unione Europea a partire dal 25 maggio 2018;

richiamato il D. Lgs. 30/06/2003, n. 196 c.d. Codice della privacy, considerato il referente normativo principale della materia, profondamente modificato con il D. Lgs. 10/08/2018 n. 101, con il quale si è armonizzata la normativa interna con quella sovranazionale, in attuazione della delega contenuta nell'art. 13 Legge 25 ottobre 2017 n. 166 (legge di delegazione europea 2016/2017).

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.

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, e' 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 Responsabile dell' Area Affari Generali 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:

- il D. Lgs. 267/2000;
- il Regolamento UE n. 679/2016;
- le linee guida adottate dal Gruppo di Lavoro art. 29 sulla protezione dei dati;
- le indicazioni fornite dall'Autorità Garante per la Protezione dei Dati personali e dal Responsabile Protezione Dati del Comune di Canegrate.

Visto:

il parere favorevole espresso dal Responsabile Dell'Area Affari Generali in ordine alla regolarità tecnica reso ai sensi dell'art. 49 comma 1 del TUEL.

con voti unanimi favorevoli resi nella forma di legge;

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.

Con successiva votazione unanime la presente è dichiarata immediatamente eseguibile ai sensi dell'art. 134 comma 4, del D. Lgs. 267/2000.

Si allega:

- Procedura per la gestione del *Data Breach* ai sensi del Regolamento Europeo 679/2016
- Parere preventivo reso ai sensi dell'art. 49 comma 1 del TUEL

Deliberazione G.C. n. 164 del 25 NOV. 2020

Letto, approvato e sottoscritto:

IL SINDACO
F.to Roberto Colombo

IL SEGRETARIO GENERALE
F.to. Dr.ssa Teresa La Scala

CERTIFICATO DI PUBBLICAZIONE

Il sottoscritto Segretario certifica che copia della presente deliberazione, ai sensi dell'art.124 del D. Lgs. n.267/2000 viene pubblicata all'Albo Pretorio on line di questo Comune il giorno 15 DIC. 2020
e vi rimarrà per la durata di quindici giorni consecutivi.

Lì, 15 DIC. 2020

IL SEGRETARIO GENERALE
F.to. Dr.ssa Teresa La Scala

AUTENTICAZIONE

La presente copia è conforme all'originale, per uso amministrativo, ai sensi del D.P.R. 28.12.2000 n.445, art.18, composta di n. 5 fogli, di cui si omettono gli allegati.

Lì 15 DIC. 2020

IL SEGRETARIO GENERALE
Dr.ssa Teresa La Scala

CERTIFICATO DI ESECUTIVITA'

Si certifica che il presente atto è stato pubblicato nelle forme di legge all'Albo pretorio del Comune ed E' DIVENTATO ESECUTIVO in data 28 DIC. 2020 ai sensi dell'art. 134, comma 3, del Decreto Legislativo 18/8/2000 n. 267.

IL SEGRETARIO GENERALE
F.to Dr.ssa Teresa La Scala