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.

COMUNE DI CANEGRATE (MILANO)

DELIBERAZIONE DI GIUNTA COMUNALE N. **164** DEL **25/11/2020**

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

COMUNE DI CANEGRATE (MILANO)

COMUNE DI CANEGRATE

Città Metropolitana di Milano

AREA AFFARI GENERALI

Parere preventivo art. 49 e art. 147 bis comma 1 Decreto Legislativo 18 agosto 2000, n. 267

Allegato alla deliberazione n. 164 assunta in data 25 NOV. 2020

☒ GIUNTA COMUNALE ☐ CONSIGLIO COMUNALE

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

In relazione al presente atto si esprime parere favorevole di regolarità tecnica.

Canegrate,

IL RESPONSABILE AREA AFFARI GENERALI
(D.ssa Teresa La Scala)

COMUNE DI CANEGRATE (MILANO)

COMUNE DI CANEGRATE (MILANO)

Allegato alla deliberazione
G.C. n. 164 del 25/11/2020

Comune di CANEGRATE
(Città Metropolitana di Milano)
Sede: via A. Manzoni, 1 - Tel. (0331) 463811 - Telefax (0331) 401535 - Cod. fisc. e part. IVA 00835500158
www.comune.canegrate.mi.it

PROCEDURA

PER LA GESTIONE DI *DATA BREACH*

AI SENSI DEL GDPR (REGOLAMENTO EUROPEO 679/2016)

Approvata con deliberazione di Giunta Municipale n. _____ del _____

- Distruzione: Indisponibilità definitiva di dati personali con impossibilità di ripristino degli stessi. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati.
- Perdita: Perdita del supporto fisico di memorizzazione dei dati derivante da privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita, può riguardare anche copie od originali dei supporti contenenti i dati personali dei soggetti interessati, ed anche se temporanea può essere potenzialmente dannosa.
- Modifica: Modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso.
- Rivelazione: Distribuzione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.
- Accesso: Accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.

2.3 Esempi di eventi che possono generare violazione di dati

Al fine di facilitare l'individuazione di una possibile violazione, vengono di seguito indicati in maniera esemplificativa e non esaustiva, una serie di possibili eventi che potenzialmente possono generare violazioni dei dati personali. Pertanto si può essere in presenza di un *data breach* anche nel caso di un evento non compreso nell'elenco di seguito riportato, di contro il verificarsi di uno degli eventi che seguono non costituisce condizione sufficiente per stabilire l'effettivo *data breach*. Il titolare deve infatti procedere sempre alle opportune valutazioni.

2.3.1 Eventi riguardanti trattamenti elettronici:

a) Eventi accidentali: Eventi anomali determinati da fatti fortuiti che causano la perdita delle caratteristiche di sicurezza dei dati personali dei clienti (confidenzialità, integrità o disponibilità) in caso di trattamenti informatizzati. Rientrano in tali casistiche eventi generati nella gestione dei sistemi ICT (gestiti internamente oppure in outsourcing) quali:

   - Esecuzione erronea di comandi e/o procedure per distrazione: ad esempio pubblicazione erronea delle informazioni personali (non di dominio pubblico) su portali web pubblici; erroneo invio di informazioni a enti esterni alla Società, formattazione di dispositivi di memorizzazione, errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi; divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato ecc.
   - Rottura delle componenti HW: a titolo di esempio distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.
   - Malfunzionamenti Software: ad esempio esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.
   - Visibilità errata di dati sul sito web dell'Ente: ad esempio visibilità di dati di altri utenti anche per casi di omonimia.
   - Fornitura dati a persona diversa dall'interessato: a titolo di esempio comunicazioni di dati di interessati a destinatari errati; gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato;
   - Guasti alla rete: a titolo di esempio caduta delle comunicazioni durante il trasferimento di

o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi dell'ente, dei collaboratori esterni. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.

- Furto (cartacei): Furto da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati dei soggetti interessati.

3. Notifica della violazione all'autorità di controllo

3.1 Quando è richiesta la notifica

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che la valutazione della violazione non evidenzi rischi per i diritti e le libertà delle persone fisiche.

Il titolare del trattamento viene considerato "a conoscenza" della violazione nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione di dati personali.

Nei casi in cui la violazione non sia evidente e chiara il titolare è tenuto ad attivare tempestivamente le indagini finalizzate a valutare se l'incidente abbia causato una effettiva violazione di dati personali, ad adottare le dovute misure correttive e ad effettuare la notifica, se ritenuta necessaria.

La notifica all'autorità di controllo effettuata oltre le 72 ore, deve essere corredata dai motivi del ritardo.

Ogni singola violazione costituisce un incidente segnalabile con rispettiva notifica; fa eccezione il caso della notifica "cumulativa" da utilizzare in presenza di violazioni multiple riguardanti il medesimo tipo di dati personali violati nel medesimo modo ed in un lasso di tempo relativamente breve.

Contrariamente, diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, costituiscono separate notifiche per ogni violazione conformemente all'articolo 33.

L'articolo 33, paragrafo 4, afferma che *"qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo"*.

Il titolare quindi, a seconda della natura e delle complessità della violazione, può effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente.

In questi casi il titolare provvede tempestivamente (entro le 72 ore) alla notifica all'autorità riservandosi di fornire informazioni supplementari in un secondo momento, si procede pertanto ad una notifica per fasi.

Se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento informa l'autorità di controllo.

L'incidente, in questo caso, viene registrato come un evento che non costituisce una violazione.

3.2. Quando non è richiesta la notifica

Quando dalla valutazione risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche il titolare non procede né alla notifica all'autorità di controllo né ad informare la persona interessata.

Nel caso in cui lo stato di assenza di un rischio probabile ai diritti ed alle libertà delle persone fisiche cambi nel corso del tempo si procede alla rivalutazione del rischio al fine di verificare se i nuovi elementi emersi rientrino nell'obbligo di notifica.

4. Contitolari del trattamento

In caso di presenza di contitolari del trattamento, il rispetto agli obblighi di notifica delle violazioni previsti dal GDPR, si fa rinvio agli accordi contrattuali che dovranno obbligatoriamente contenere

registrazioni dei dati personali in questione (Le categorie di registrazioni dei dati personali fanno riferimento ai diversi tipi di registrazioni di cui il titolare del trattamento può disporre, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.) ;

- 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.

L'impossibilità da parte del titolare di disporre di informazioni precise (ad esempio il numero esatto di interessati coinvolti) non costituisce un ostacolo alla notifica tempestiva delle violazioni; in questo caso la comunicazione deve contenere un'approssimazione sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte.
Le informazioni sopra indicate costituiscono il contenuto minimo della notifica, è facoltà del titolare del trattamento, qualora lo ritenga necessario, fornire ulteriori informazioni.

8. Comunicazione all'interessato

Ai sensi dell'articolo 34, paragrafo 1, *"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"*.

8.1 Contenuto della comunicazione

La comunicazione di una violazione agli interessati deve avvenire senza ingiustificato ritardo e, deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali e deve contenere 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.

8.2 Modalità della comunicazione

La violazione va comunicata direttamente agli interessati coinvolti.
Nel caso la comunicazione diretta non risulta percorribile si procede ad una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c); la misura più efficace, valutata la fattispecie concreta, viene stabilita dal titolare.
Il titolare, può contattare l'autorità di controllo per chiedere indicazioni ed orientamenti in merito all'opportunità di informare gli interessati sulla violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli. Qualora il titolare non sia in possesso di dati sufficienti per contattare l'interessato procede ad informarlo non appena sia ragionevolmente possibile (ad esempio può accadere che il titolare entra in possesso di dati necessari per contattare l'interessato nel momento in cui lo stesso esercita il proprio diritto di accesso ai dati ai sensi dell'articolo 15).

- Caratteristiche particolari del titolare del trattamento di dati: valutare la natura e il ruolo del titolare del trattamento e delle sue attività che possono influire sul livello di rischio per le persone fisiche in seguito a una violazione.
- Numero di persone fisiche interessate : valutare il numero di persone fisiche coinvolte nella violazione.

10. Registro delle violazioni

E' istituito un registro interno delle violazioni dove vengono annotate sia le violazioni non notificabili che quelle notificabili.
In ossequio al principio di responsabilizzazione di cui all'articolo 5 paragrafo 2, il titolare del trattamento conserva la documentazione di tutte le violazioni come stabilito all'articolo 33, paragrafo 5: *"Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo ".*

Il registro 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);

Il titolare conserva la documentazione in conformità dell'articolo 33, paragrafo 5, anche al fine di poter fornire prontamente le prove dall'autorità di controllo in caso di suo intervento.

11. Gestione del *data breach* - Istituzione "Gruppo Privacy"

E' istituito il "Gruppo Privacy", (di seguito "Gruppo").
Al fine di garantire una adeguata presenza delle competenze necessarie alla gestione del data breach il Gruppo è formato dal Responsabile del Settore Affari Generali e dal Responsabile Settore Servizi Telematici e Digitalizzazione.
Il Gruppo opera in stretta correlazione e collaborazione con il Responsabile di Protezione Dati e si conforma, nelle azioni da intraprendere, a tutte le sue indicazioni e prescrizioni. Nella gestione della violazione, inoltre il Gruppo si avvale durante l'intero processo anche del Responsabile del Settore a cui fa capo il dato o il gruppo di dati violati.

Al Gruppo sono assegnate le seguenti competenze:

- la predisposizione e l'invio della notifica della violazione all'autorità di controllo utilizzando il modello messo a disposizione sul sito del Garante della Privacy all'indirizzo https://www.garanteprivacy.it o tramite pec all'indirizzo
- protocollo@pec.gpdp.it:
  - la valutazione del rischio e l'attivazione di eventuali indagini sulla violazione;
  - l'invio all'autorità di controllo di eventuali informazioni supplementari riguardanti la segnalazione già resa;
  - la comunicazione agli interessati,
  - la tenuta del Registro delle violazioni.

Il Gruppo, valutata la fattispecie concreta, individua all'occorrenza personale tecnico e/o amministrativo necessario stabilmente o episodicamente alle attività da svolgere; dell'individuazione

Premessa

Il Regolamento Europeo sulla protezione dei dati n. 679/2016 (di seguito "GDPR"), entrato in vigore definitivamente il 25 maggio 2018, 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.
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.
Il GDPR impone al titolare di disporre le misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati al fine di proteggerli dalle violazioni sopra descritte.
Il presente documento si prefigge lo scopo di indicare le modalità di gestione del *data breach* garantendone la realizzabilità tecnica e la sostenibilità organizzativa.
La presente procedura viene approvata dalla Giunta Municipale con propria deliberazione; compete allo stesso organo definire eventuali modifiche o integrazioni.
Al fine di garantirne la massima diffusione interna ed esterna e la massima conoscibilità sulle azioni da intraprendere e sui comportamenti da adottare in caso di *data breach* la presente viene comunicata a tutti i dipendenti dell'Ente dopo la sua approvazione e resa disponibile sul sito web istituzionale nella sezione "Amministrazione Trasparente", sottosezione di primo livello "Altri Contenuti", sottosezione di secondo livello "Privacy".

1. Normativa e documenti di riferimento

Regolamento HE 679/2016 ("GDPR")
Dlgs 196/2003 come modificato dal D.Lgs 101/2018;
Piano di Protezione dei dati Personali e Gestione del rischio di violazione approvato con deliberazione di Giunta Municipale n. _____ del _____

2. Definizione di violazione dei dati:

2.1 Classificazione delle violazioni:

Le violazioni si classificano nel seguente modo:

- violazione della riservatezza: in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- violazione dell'integrità : in caso di modifica non autorizzata o accidentale dei dati personali;
- violazione della disponibilità: in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

La violazione può riguardare la riservatezza, l'integrità, la disponibilità dei dati personali o qualsiasi combinazione delle stesse.
Al fine di adottare le corrette procedure di segnalazione è di fondamentale importanza sapere identificare una violazione, saperne valutare la natura e le potenziali conseguenze negative.
Le violazioni dei dati personali si considerano tali se hanno un reale impatto sulla confidenzialità, integrità o disponibilità dei dati personali degli interessati (cittadini, dipendenti, soggetti terzi ecc).

2.2 Tipologie di violazioni

All'interno della classificazione sopra indicata, quindi, si possono avere le seguenti tipologie di violazione dei dati personali:

dati e perdita di dati durante la trasmissione, ecc.

b) Eventi dolosi: eventi dolosi causati da personale interno o soggetti esterni realizzati tramite: accesso non autorizzato ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione; compromissione o rivelazione abusiva di credenziali di autenticazione; utilizzo di software malevolo. In tale casistica rientrano gli incidenti di sicurezza ICT che comportano la violazione dei dati personali quali:

- Furto: furto di supporti di memorizzazione e/o elaborazione contenenti dati personali dei clienti;
- Truffa informatica esterna: tutti i casi di frodi realizzate da un soggetto esterno dell'Ente rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente o da suoi fornitori. Ad esempio: accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi;
- appropriazione dei dati di carta di credito; appropriazione (e diffusione) delle credenziali di autenticazione ai servizi dei clienti.
- Truffa informatica interna: tutti i casi di frodi realizzate da personale interno all'Ente che comportano la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

2.3.2 Eventi riguardanti trattamenti cartacei

a) Eventi accidentali: Eventi anomali causati nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei dei dati personali dei clienti dell'ente quali:

- Distruzione accidentale di documenti: ad esempio incendio/ allagamento dei locali dove sono presenti archivi cartacei, causati da eventi fortuiti e non dolosi presso le sedi dell'ente e dei locali, degli outsourcers di archiviazione contratti, dei collaboratori cessati dai quali si attende la restituzione della documentazione contrattuale;
- Distruzione per errore di documenti originali, senza eventuale copia, da parte di dipendenti interni, di collaboratori esterni;
- Smarrimento di documenti: ad esempio perdita di documenti contenenti dati dei cittadini, degli outsourcers (es. archiviazione contratti).
- Fornitura involontaria di dati a persona diversa dal contraente: ad esempio invio lettera ad Ente senza mandato, gestione ed evasione reclami/richieste di informazioni avanzate da persone diverse dal titolare della linea non delegato, comunicazione di dati dal subentrato al subentrante e viceversa, invio/visualizzazione di fatture a soggetti diversi dagli autorizzati.

b) Eventi dolosi: Comportamenti dolosi da parte di personale interno o soggetti esterni realizzati, attraverso accessi non autorizzati, nell'ambito di trattamenti effettuati su archivi cartacei di dati personali del Comune quali:

- Distruzione dolosa dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati dell'utenza; accesso non autorizzato da parte di terzi ad archivi interni della Società e distruzione volontaria di documenti contenenti dati dell'utenza.
- Accesso non autorizzato: ad esempio accesso non autorizzato da parte di personale interno

l'indicazione del titolare responsabile delle violazioni e della eventuale notifica all'autorità di controllo.

5. Responsabile del trattamento

Il responsabile del trattamento svolge un ruolo importante nel consentire al titolare del trattamento di adempiere ai propri obblighi in materia di notifica delle violazioni.
Il contratto, o altro atto giuridico, che disciplina il rapporto tra il titolare ed il responsabile del trattamento deve contenere la seguente previsione *"Il responsabile del trattamento assiste il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento"*.
Se il responsabile del trattamento viene a conoscenza di una violazione dei dati personali che sta trattando per conto del titolare del trattamento, deve notificarla al titolare del trattamento senza ingiustificato ritardo e comunque non oltre le 24 ore.
La valutazione del rischio derivante dalla violazione spetta al titolare del trattamento nel momento in cui viene a conoscenza della violazione; in capo al responsabile del trattamento insiste esclusivamente l'obbligo di verificare l'esistenza di una violazione e di notificarla tempestivamente al titolare del trattamento nei tempi sopra indicati.
In considerazione del fatto che ai sensi del GDPR la responsabilità legale della notifica rimane sempre in capo al titolare del trattamento, il responsabile del trattamento può effettuare la notifica della violazione per conto del titolare esclusivamente nel caso in cui quest'ultimo gli abbia conferito apposita autorizzazione e/o nel caso in cui tale modalità sia espressamente prevista negli accordi contrattuali tra i due soggetti. In caso contrario è fatto obbligo al responsabile del trattamento di informare il titolare, nelle modalità e nei tempi di cui sopra, di ogni potenziale evento di data breach.
La segnalazione può essere trasmessa via PEC all'indirizzo comune.canegrate@pec.regione.lombardia.itoviae-mail oppure all'indirizzo protocollo@comune.canegrate.mi.it.

Delle seguenti prescrizioni è fatta apposita menzione nel contratto, o altro atto giuridico, che disciplina il rapporto tra il titolare ed il responsabile del trattamento.

6. Responsabile della protezione dati (RPD)

Il Responsabile della Protezione dati (di seguito "RPD") fornisce consulenza e informazioni al titolare del trattamento e/o al responsabile del trattamento in merito alla valutazione della necessità di notificare una violazione. L'RPD coopera inoltre con l'autorità di controllo e funge da punto di contatto per l'autorità di controllo e per gli eventuali interessati.
Il RPD viene informato tempestivamente dell'esistenza di una violazione e viene coinvolto nell'intera gestione delle violazioni, nonché nel processo di notifica.
Il RPD, quindi, svolge un ruolo di assistenza nella prevenzione delle violazioni, fornisce consulenza e monitora il rispetto delle norme durante il processo di gestione della violazione e assiste l'Ente nell'eventualità di successive indagini da parte dell'autorità di controllo.
Il RPD, inoltre, su richiesta del titolare del trattamento, esprime pareri in merito alla struttura, all'impostazione, all'amministrazione ed alla conservazione della documentazione relativa al registro delle violazioni.

7. Contenuti della notifica: informazioni obbligatorie da fornire all'autorità di controllo

La notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- descrizione della natura della violazione dei dati personali (compresi, ove possibile, le categorie e il numero degli interessati (persone fisiche i cui dati personali sono stati oggetto di violazione) e le

8.3 Quando la comunicazione non deve essere effettuata

La comunicazione agli interessati in caso di violazione dei dati non deve essere effettuata, ai sensi dell'articolo 34 paragrafo 3, se si verifica una delle seguenti tre condizioni:

- Il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione tali rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura);
- Subito dopo la violazione il titolare ha adottato una serie di misure che rendano improbabile l'elevato rischio posto ai diritti e alle libertà delle persone fisiche (es. l'immediata azione nei confronti del soggetto che ha avuto accesso ai dati personali in modo da inibirne qualsiasi utilizzo);
- Contattare gli interessati richiede uno sforzo sproporzionato. In tale circostanza il titolare provvede ad effettuare una comunicazione pubblica o individua una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace.

Seppure la violazione inizialmente non rilevi necessità di una comunicazione all'interessato per l'assenza di rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe nel tempo subire delle variazioni, pertanto il titolare rivaluta il rischio e provvede all'eventuale comunicazione nelle modalità di cui sopra.

8.4 Quando la comunicazione va sempre effettuata

Il titolare provvede in qualunque caso alla comunicazione nel caso in cui questa venga richiesta direttamente all'autorità di controllo al fine di evitare da parte della stessa l'esercizio dei poteri sanzionatori.

9. Valutazione del rischio

Non appena il titolare del trattamento viene a conoscenza di una violazione oltre a mettere in campo tutte le azioni necessarie a contenere l'incidente, valuta anche il rischio che potrebbe derivarne.
Il rischio viene valutato in base a criteri oggettivi; i considerando 75 e 76 stabiliscono che la valutazione deve tenere conto della probabilità e della gravità del rischio per i diritti e le libertà degli interessati.
La valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati (DPIA). La valutazione di impatto prende in considerazione infatti un evento ipotetico; nel caso invece di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione va concentrata esclusivamente sul rischio risultante dell'impatto di tale violazione sulle persone fisiche.

La valutazione viene effettuata tenendo conto dei seguenti criteri:

- Tipo di violazione: valutare se la violazione può influire sul livello di rischio per persone fisiche;
- Natura, carattere sensibile e volume dei dati personali: valutare il carattere, il tipo ed il volume dei dati violati.
- Facilità di identificazione delle persone fisiche: valutare la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche.
- Gravità delle conseguenze per le persone fisiche: valutare il grado di gravità del danno potenziale che la violazione potrebbe creare alle persone.
- Caratteristiche particolari dell'interessato: valutare attentamente se la violazione riguardi dati personali relativi a minori o ad altre persone fisiche vulnerabili che possono essere soggette a un rischio più elevato di danno.

viene dato riscontro in apposito verbale.
Tutti i dipendenti comunali autorizzati a trattare dati, possono potenzialmente venire a conoscenza di un *data breach,* al verificarsi di tale evento è fatto obbligo di avvisare tempestivamente il Responsabile del Settore in qualità di Designato dal Titolare al trattamento dati.
Quest'ultimo, valutato l'evento alla luce delle indicazioni sopra fomite, qualora rilevi caratteristiche riconducibili ad un potenziale *data breach*, in considerazione dei ristretti tempi di azione e della potenziale gravità delle conseguenze, ha l'obbligo di segnalarlo tempestivamente utilizzando l'apposita e-mail (**casella di posta da individuare**) e contemporaneamente, per garantire l'immediata gestione della segnalazione, comunicare l'evento anche per le vie brevi attraverso i recapiti telefonici interni (**da individuare successivamente**).
Il Gruppo, avvalendosi del supporto del RPD, se rileva che l'episodio può essere classificato come *data breach*, predispone la comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, nelle modalità sopra indicate.
Il Gruppo provvede ad annotare sul registro le eventuali ragioni del ritardo della notifica effettuata oltre le 72 ore, nonché le motivazioni ed il ragionamento che hanno portato a non notificare una violazione.

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. 16 fogli.

Lì 15 DIC. 2020

COMUNE DI CANEGRATE (MILANO)

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 _____ 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