CITTÀ DI SANTENA

Città Metropolitana di Torino

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N.26

OGGETTO:

Approvazione procedura per la gestione di data breach e istituzione registro data breach ai sensi del regolamento (UE) n.679/2016.

L'anno **duemilaventitre** addì **trenta** del mese di **marzo** alle ore **diciannove** e minuti **zero**, regolarmente convocata, si è riunita la Giunta comunale. Partecipa in videoconferenza l'Ass. Alessia Perrone e sono presenti per la trattazione dell'argomento in oggetto i signori:

Cognome e Nome	Carica	Presente
1. GHIO Roberto	Sindaco	Sì
2. SICILIANO Concetta	Assessore	Giust.
3. ROMANO Paolo	Vice Sindaco	Sì
4. BARBINI Cristian	Assessore	Sì
5. PERRONE Alessia	Assessore	Sì
6. TRIMBOLI Ugo Cosimo	Assessore	Sì
Totale Presenti:		5
Totale Assenti:		1

Con la partecipazione del Segretario Generale Dott. Pietrantonio DI MONTE la Giunta comunale ha assunto la deliberazione di cui all'interno.

Riconosciuto legale il numero degli intervenuti, il Sindaco GHIO Roberto assume la presidenza e dichiara aperta la seduta per la trattazione dell'argomento indicato in oggetto.

CITTÀ DI SANTENA

Città Metropolitana di Torino

Deliberazione della Giunta Comunale avente ad oggetto: **Approvazione procedura per la gestione di data breach e istituzione registro data breach ai sensi del regolamento (UE) n.679/2016.**

RILEVATO CHE la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è 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:

1. la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
2. 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;
3. 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- General Data Protection Regulation, 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;

CITTÀ DI SANTENA

Città Metropolitana di Torino

DATO ATTO CHE la notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

1. descrizione della natura della violazione dei dati personali e le registrazioni dei dati personali in questione;
2. 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;
3. descrizione delle probabili conseguenze della violazione dei dati personali;
4. 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:

1. il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
2. una descrizione delle probabili conseguenze della violazione;
3. 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:
    a. i dettagli relativi alla violazione (cause, fatti e dati personali interessati);
    b. gli effetti e le conseguenze della violazione;
    c. i provvedimenti adottati per porvi rimedio;
    d. 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 occorre procedere alla approvazione della "***Procedura per la gestione di data breach***" ai sensi del Regolamento (UE) n.679/2016, comprensivo delle seguenti schede:

a. Schede di raccolta dati- segnalazione (*Modulo DB01 – Prima Segnalazione)* utilizzato dall'operatore dell'Ente che rileva la violazione dei dati personali).

b. Scheda raccolta dati identificativi della violazione (*Modulo DB02 – Identificazione Evento)* utilizzato dall'Incaricato alla gestione delle violazioni per la valutazione di primo livello.
c. Scheda analisi evento (*Modulo DB03 – Analisi Evento*) utilizzato dal Gruppo di Gestione della Violazione per la valutazione di secondo livello, di dettaglio della violazione.
d. Scheda segnalazione all'interessato (*Modulo DB04 – Segnalazione interessato*) utilizzato dal Gruppo di Gestione della Violazione per la comunicazione agli interessati.
e. Scheda esplicativa della gestione: *Guida per la gestione delle violazioni di dati personali* - Data Breach, utilizzato dall' Incaricato alla Gestione delle Violazioni nella fase di classificazione degli accadimenti e nella compilazione del *Modulo DB02 – Identificazione Evento.*
f. Scheda guida alla valutazione delle violazioni (*Modulo Data Brench guida valutazione*) utilizzato per la corretta identificazione e gestione delle violazioni.

DATO ATTO ALTRESÌ che si rende necessario procedere all'istituzione del relativo "***Registro per la registrazione di tutte le violazioni***", allegato alla presente, per formarne parte integrante e sostanziale;

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 Comune di SANTENA, ha individuato quale responsabile del procedimento, la figura della Responsabile Area 1 Finanze - Catia CAMPACI, dipendente dell'Ente, 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 sul Sistema dei 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 (Working Party 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- 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;

VISTO il parere tecnico favorevole espresso dal Responsabile ordine alla regolarità tecnica ed il parere favorevole espresso dal Responsabile del Area Finanziaria in ordine alla regolarità contabile del presente atto (art. 49, 1° comma, D.Lgs. 267/2000);

ad unanimità 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, comprendente le seguenti schede:
   a) Schede di raccolta dati- segnalazione (*Modulo DB01 – Prima Segnalazione)* utilizzato dall'operatore dell'Ente che rileva la violazione dei dati personali).
   b) Scheda raccolta dati identificativi della violazione (*Modulo DB02 – Identificazione Evento)* utilizzato dall'Incaricato alla gestione delle violazioni per la valutazione di primo livello.

c) Scheda analisi evento (*Modulo DB03 – Analisi Evento*) utilizzato dal Gruppo di Gestione della Violazione per la valutazione di secondo livello, di dettaglio della violazione.
d) Scheda segnalazione all'interessato (*Modulo DB04 – Segnalazione interessato*) utilizzato dal Gruppo di Gestione della Violazione per la comunicazione agli interessati.
e) Scheda esplicativa della gestione: *Guida per la gestione delle violazioni di dati personali* - Data Breach, utilizzato dall' Incaricato alla Gestione delle Violazioni nella fase di classificazione degli accadimenti e nella compilazione del *Modulo DB02 – Identificazione Evento.*
f) Scheda guida alla valutazione delle violazioni (*Modulo Data Brench guida valutazione*) utilizzato per la corretta identificazione e gestione delle violazioni;

2. **DI APPROVARE ALTRESÌ** l'istituzione del relativo "***Registro per la registrazione di tutte le violazioni***" ai sensi del Regolamento (UE) n.679/2016;

3. **DI DARE ATTO** che il Responsabile del Procedimento è il Responsabile Area 1 Finanze - Catia CAMPACI;

4. **DI DISPORRE** che al presente provvedimento venga assicurata:
a) la pubblicità legale con pubblicazione all'Albo Pretorio;
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";

5. **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;

6. **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;

CITTÀ DI SANTENA

Città Metropolitana di Torino

Successivamente,

LA GIUNTA COMUNALE

Stante l'urgenza di poter attivare con tempestività le procedure amministrative successive all'adozione del presente atto;

Con voti unanimi e favorevoli espressi nelle forme di legge,

DELIBERA

Di dichiarare il presente provvedimento immediatamente eseguibile ai sensi dell'art. 134, comma 4, del D.lgs. n. 267/2000 per consentire l'adozione immediata degli adempimenti conseguenti.

Del che si è redatto il presente verbale.

IL SINDACO
Firmato digitalmente
F.to: GHIO Roberto

IL SEGRETARIO GENERALE
Firmato digitalmente
F.to: Dott. Pietrantonio DI MONTE