C I T T A ’ D I F E R M O

ATTO DI GIUNTA DEL 17-09-2024, n. 327

COPIA

Oggetto:
Approvazione Piano di protezione dei dati personali e di gestione del rischio di violazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016

L'anno duemilaventiquattro nel giorno diciassette del mese di settembre alle ore 16:25 si e' riunita in una sala del Comune, previo regolare invito, la Giunta con l'intervento dei Signori:

Calcinaro Paolo	**SINDACO**	**Presente**
Torresi Mauro	**VICE SINDACO**	**Presente**
Giampieri Mirco	**ASSESSORE**	**Presente**
Di Felice Mariantonietta	**ASSESSORE**	**Presente**
Cerretani Annalisa	**ASSESSORE**	**Presente**
Luciani Ingrid	**ASSESSORE**	**Presente**
Ciarrocchi Alessandro	**ASSESSORE**	**Presente**
Scarfini Alberto Maria	**ASSESSORE**	**Presente**
Lanzidei Micol	**ASSESSORE**	**Presente**

Risultano presenti n. 9 e assenti n. 0

Presiede il SINDACO Avv. Calcinaro Paolo
Assiste il Segretario Generale Dott. Vesprini Dino.

Il Presidente, accertato il numero legale, dichiara aperta la seduta ed invita la Giunta Comunale ad esaminare e ad assumere le proprie determinazioni sulla proposta indicata in oggetto.

Alla 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.

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 divenuto 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;

Richiamata la Legge 25 ottobre 2017, n. 163 e, in particolare, l'art. 13, che ha delegato il Governo per l'adeguamento della normativa nazionale alle disposizioni del GDPR;

Rilevato che il successivo decreto legislativo delegato, D.Lgs. 101/2018, ha inteso realizzare l'adeguamento sulla base dei seguenti *principi e criteri direttivi* specifici:

a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;
b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;
c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;
d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;

e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse;

Dato atto che, sulla base del delineato quadro normativo, l'obiettivo di fondo del GDPR è la sicurezza del trattamento dei dati personali, programmando e pianificando gli interventi affinché i dati personali siano:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatto salvo l'adeguamento di misure tecniche e organizzative adeguate richieste dal presente GDPR a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Ritenuto che l'obiettivo di assicurare la sicurezza dei dati richiede di gestire efficacemente, e conformemente alle disposizioni del GDPR, il rischio di violazione dei dati derivante dal trattamento, per tale dovendosi intendere 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 e che, a tal fine, vadano definiti gli obiettivi correlati alla gestione del rischio;

Considerato che nel testo normativo del GDPR la parola "rischio" compare circa 70 volte e che quindi , su indicazione e con il supporto dello stesso RPD dell'ente, appare opportuno

garantire la protezione richiesta facendo ricorso ai modelli più aggiornati del Risk Management, oggi formalizzati nello standard UNI ISO 31000, applicandone i principi e le linee guida contenute ;

Considerato, altresì, che la citata norma UNI ISO 31.000 contiene l'indicazione di predisporre e di attuare *Piani di trattamento del rischio* e di documentare, secondo il *principio di tracciabilità documentale*, come le opzioni di trattamento individuate che sono state attuate;

Ritenuto, pertanto, necessario procedere alla approvazione di un piano di protezione dei dati personali e di gestione del rischio di violazione

Visto l'allegato schema di Piano;

Appurato che:

- lo schema di piano copre il periodo del triennio **2024-2026**
- la funzione principale dello stesso è quella di assicurare il processo, a ciclo continuo, di adozione, modificazione, aggiornamento e adeguamento del processo di gestione del rischio e della strategia di sicurezza, secondo i principi, le disposizioni e le linee guida elaborate a livello nazionale e internazionale;
- il documento consente che la strategia si sviluppi e si modifichi in modo da mettere via via a punto degli strumenti di protezione mirati e sempre più incisivi;
- l'adozione del documento non si configura come un'attività una tantum, bensì come un processo continuo in cui le strategie e gli strumenti vengono via via affinati, modificati o sostituiti in relazione al feedback ottenuto dalla loro applicazione;
- eventuali aggiornamenti successivi, anche infra annuali, correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD, sono oggetto di approvazione da parte dello stesso organo che ha approvato il PPD;

Considerato che lo schema di Piano è stato predisposto dal responsabile del procedimento con il coinvolgimento e la partecipazione degli attori indicati nello Schema di Piano medesimo e, in particolare con li coinvolgimento del responsabile dei sistemi informativi;

Rilevato che il Responsabile del procedimento è il Dirigente del Settore I Contenzioso, Accesso agli Atti, Privacy e Transizione Digitale

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;

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate, si propone

1. Di approvare l'allegato schema di "Piano di protezione dei dati personali e di gestione del rischio di violazione", comprensivo di n. 9 allegati disponibili in atti, numerati dal n.1 al n.9, di cui il solo n.9 a titolo "Programmazione Corsi di Formazione" soggetto a pubblicazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016;

2. Di dare atto che il Piano copre il periodo di un triennio, 2024-2026 ed è soggetto ad aggiornamento annuale, e ad aggiornamenti anche infrannuali correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD;

3. Di comunicare i contenuti del Piano a tutti i soggetti indicati nel Piano medesimo, attraverso i canali dallo stesso individuati,.

4. 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 nella sezione "Amministrazione trasparente", sezione Privacy;

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.

Oggetto: **Approvazione Piano di protezione dei dati personali e di gestione del rischio di violazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016**

Pareri espressi ai sensi dell'art. 49 D.Lgs. 18/08/2000 n. 267:

Fermo, 17/09/2024

Parere di regolarità tecnica: favorevole
Il Dirigente Settore I Contenzioso, Accesso agli Atti, Privacy e Transizione Digitale
Dott. Francesco Michelangeli

Fermo, 17/09/2024

Visto di conformità dell'azione amministrativa
Il Segretario Generale

Dott. Dino Vesprini

La Giunta Comunale

Visto il documento istruttorio sopra riportato;

Visto il parere favorevole espresso dal competente Dirigente di Settore, in qualità di Responsabile, in ordine alla regolarità tecnica, ai sensi dell'art, 49 del D.Lgs. 267/2000, nonché il visto di conformità dell'azione amministrativa espresso dal Segretario Generale;

Con voti favorevoli unanimi, resi ed accertati in forma palese

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

Delibera

1. Di approvare l'allegato schema di "Piano di protezione dei dati personali e di gestione del rischio di violazione", comprensivo di n. 9 allegati disponibili in atti, numerati dal n.1 al n.9, di cui il solo n.9 a titolo "Programmazione Corsi di Formazione" soggetto a pubblicazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016;

2. Di dare atto che il Piano copre il periodo di un triennio, 2024-2026 ed è soggetto ad aggiornamento annuale, e ad aggiornamenti anche infrannuali correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD;

3. Di comunicare i contenuti del Piano a tutti i soggetti indicati nel Piano medesimo, attraverso i canali dallo stesso individuati,.

4. Di disporre che al presente provvedimento venga assicurata:

c) la pubblicità legale con pubblicazione all'Albo Pretorio
nonché
d) la trasparenza mediante la pubblicazione sul sito web istituzionale nella sezione "Amministrazione trasparente", sezione Privacy.

****

La presente deliberazione, per ragioni di urgenza, con separata e successiva votazione unanime, è dichiarata immediatamente eseguibile ai sensi e per gli effetti dell'art. 134, comma 4 del T.U. delle leggi sull'ordinamento degli enti locali, D.lgs. 18/08/2000 n. 267.

Letto, approvato e sottoscritto

IL SINDACO
F.to Avv. Calcinaro Paolo

Il Segretario Generale
F.to Dott. Vesprini Dino

CERTIFICATO DI PUBBLICAZIONE

Si certifica che il presente atto è pubblicato all'Albo Pretorio di questo Comune, in data odierna per quindici giorni consecutivi.

Fermo, lì

Il Segretario Generale
F.to Dott. Vesprini Dino

E' copia conforme all'originale

Fermo, lì _____

L'impiegato addetto

CERTIFICATO DI ESECUTIVITA'

Il presente atto è esecutivo:

- ❑ Dopo il decimo giorno dalla data di pubblicazione sopra indicata.

- ❑ Lo stesso giorno in cui l'atto è stato adottato.

Fermo, lì _____

Il Segretario Generale
F.to Dott. Vesprini Dino