# CITTA' DI TREIA
(Provincia di Macerata)

*Cod. COM. 43054*

## COPIA DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Numero 149 del 05-09-2018

**Oggetto:** **DEFINIZIONE DEGLI OBIETTIVI STRATEGICI IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NELL'AMBITO DELLE MISURE FINALIZZATE A DARE ATTUAZIONE ALLE DISPOSIZIONI DEL REGOLAMENTO (UE) N. 679/2016.**

Il giorno **cinque settembre duemiladiciotto**, alle ore **13:45**, nella Residenza municipale, in seguito a convocazione disposta nei modi di legge, si è riunita la Giunta comunale nelle persone dei Signori:

| Nominativo | Carica | Pres. / Ass. |
|---|---|---|
| CASTELLANI EDI | VICESINDACO | P |
| SAVI ALESSIA | ASSESSORE | P |
| BUSCHITTARI DAVID | ASSESSORE | P |
| MORETTI LUANA | ASSESSORE | P |

**presenti n. 4 assenti n. 0**

Partecipa, con funzioni esecutive, referenti e di assistenza e ne cura la verbalizzazione (articolo 97, comma 4a, del D.Lgs. n. 267/2000) il Segretario Comunale **PERRONI BENEDETTO**.

Il **Vicesindaco**, **CASTELLANI EDI,** constatato il numero legale degli intervenuti, pone in discussione la pratica segnata all'ordine del giorno:

**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;

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

**RILEVATO** che il decreto legislativo delegato è finalizzato a 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;

**RITENUTO** che l'imminente adeguamento dell'ordinamento nazionale interno al GDPR renda necessario definire le politiche e gli obiettivi strategici da conseguire per garantire l'adeguamento;

**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;

**DATO ATTO** che tali obiettivi possono essere individuati nel gestire il rischio di violazione dei dati applicando i principi e le linee guida contenute nella norma UNI ISO 31.000 secondo cui:

a) *La gestione del rischio crea e protegge il valore*. La gestione del rischio contribuisce in maniera dimostrabile al raggiungimento degli obiettivi ed al miglioramento della prestazione, per esempio in termini di salute e sicurezza delle persone, security, rispetto dei requisiti cogenti, consenso presso l'opinione pubblica, protezione dell'ambiente, qualità del prodotto, gestione dei progetti, efficienza nelle operazioni, governance e reputazione.

b) *La gestione del rischio è parte integrante di tutti i processi dell'organizz*azione. La gestione del rischio non è un'attività indipendente, separata dalle attività e dai processi principali dell'organizzazione. La gestione del rischio fa parte delle responsabilità della direzione ed è parte integrante di tutti i processi dell'organizzazione, inclusi la pianificazione strategica e tutti i processi di gestione dei progetti e del cambiamento.

c) *La gestione del rischio è parte del processo decisionale*. La gestione del rischio aiuta i responsabili delle decisioni ad effettuare scelte consapevoli, determinare la scala di priorità delle azioni e distinguere tra linee di azione alternative.

d) *La gestione del rischio tratta esplicitamente l'incertezza*. La gestione del rischio tiene conto esplicitamente dell'incertezza, della natura di tale incertezza e di come può essere affrontata.

e) *La gestione del rischio è sistematica, strutturata e tempestiva*. Un approccio sistematico, tempestivo e strutturato alla gestione del rischio contribuisce all'efficienza ed a risultati coerenti, confrontabili ed affidabili.

f) *La gestione del rischio si basa sulle migliori informazioni disponibili*. Gli elementi in ingresso al processo per gestire il rischio si basano su fonti di informazione quali dati storici, esperienza, informazioni di ritorno dai portatori d'interesse, osservazioni, previsioni e parere di specialisti. Tuttavia, i responsabili delle decisioni dovrebbero informarsi e tenerne conto di qualsiasi limitazione dei dati o dei modelli utilizzati o delle possibilità di divergenza di opinione tra gli specialisti.

g) *La gestione del rischio è "su misura"*. La gestione del rischio è in linea con il contesto esterno ed interno e con il profilo di rischio dell'organizzazione.

h) *La gestione del rischio tiene conto dei fattori umani e culturali*. Nell'ambito della gestione del rischio individua capacità, percezioni e aspettative delle persone esterne ed interne che possono facilitare o impedire il raggiungimento degli obiettivi dell'organizzazione.

i) *La gestione del rischio è trasparente e inclusiva*. Il coinvolgimento appropriato e tempestivo dei portatori d'interesse e, in particolare, dei responsabili delle decisioni, a tutti i livelli dell'organizzazione, assicura che la gestione del rischio rimanga pertinente ed aggiornata. Il coinvolgimento, inoltre, permette che i portatori d'interesse siano opportunamente rappresentati e che i loro punti di vista siano presi in considerazione nel definire i criteri di rischio.

l) *La gestione del rischio è dinamica*. La gestione del rischio è sensibile e risponde al cambiamento continuamente. Ogni qualvolta accadono eventi esterni ed interni, cambiano il contesto e la conoscenza, si attuano il monitoraggio ed il riesame, emergono nuovi rischi, alcuni rischi si modificano ed altri scompaiono.

m) *La gestione del rischio favorisce il miglioramento continuo dell'organizzazione.* Le organizzazioni dovrebbero sviluppare ed attuare strategie per migliorare la maturità della propria gestione del rischio insieme a tutti gli altri aspetti della propria organizzazione.

**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, di includere, negli obiettivi strategici che il titolare intende perseguire per l'anno 2018, anche l'adozione di un apposito Piano di protezione dei dati personali e di gestione del rischio di violazione;

**RILEVATO** che la presente deliberazione costituisce parte del processo amministrativo, mappato nel PTPCT quale procedimento, i cui tempi conclusivi sono oggetto di monitoraggio;

**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 azione - 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** l'articolo 4 del D.Lgs. 30 marzo 2001, n. 165;

**VISTO** l'articolo 48 del TUEL di cui al D.Lgs. 18 agosto 2000, n. 267 e successive modificazioni in ordine alla competenza della Giunta;

**ACQUISITO** il parere favorevole del Segretario Generale in ordine alla

regolarità tecnica, espresso sulla proposta della presente deliberazione ai sensi degli articoli 49, comma 1, e 147-*bis*, comma 1, del D.Lgs. n. 267/2000, come riportato e inserito in calce all'atto;

**DATO ATTO** che sulla proposta non è stato acquisito il parere del Funzionario responsabile del Servizio Finanziario ai sensi degli articoli 49, comma 1, e 147-*bis*, comma 1, del D.Lgs. n. 267/2000, in quanto la stessa nono comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'Ente, come riportato e inserito in calce all'atto;

**CON VOTI** favorevoli unanimi, espressi in forma palese;

**D E L I B E R A**

1) di **DICHIARARE** la narrativa che precede parte integrante e sostanziale del presente atto;

2) di **DEFINIRE** i seguenti obiettivi strategici in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, al fine del loro recepimento e conseguente declinazione nei vari documenti di programmazione strategico-gestionale:

| OBIETTIVI STRATEGICI | OBIETTIVI OPERATIVI |
|---|---|
| | **OBIETTIVO OPERATIVO N. 1**<br>Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, adottare le misure di adeguamento gestionale, documentale, organizzativo e procedurale nonché di aggiornamento delle conoscenze e competenze che si rivelino funzionali a garantire la conformità del trattamento al GDPR e, mettere in atto, anche mediante informatizzazione dei relativi processi gestionali, misure di sicurezza logistiche, tecniche informatiche, procedurali ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, istituendo e tenendo costantemente aggiornati i Registri delle attività e delle categorie di trattamento. |
| | **OBIETTIVO OPERATIVO N. 2**<br>Elaborare e attuare un Piano di protezione dei dati e di gestione del rischio di violazione (PPD) e documentare, secondo il principio di tracciabilità documentale, come le opzioni di trattamento individuate sono state attuate, integrando la protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, secondo le disposizioni del GDPR, nella gestione di tutti i processi gestionali, implementando la cultura della sicurezza nel contesto interno ed esterno dell'organizzazione, provvedendo, altresì, alla designazione del Responsabile della Protezione dei Dati (RPD). |
| | **OBIETTIVO OPERATIVO N. 3**<br>Garantire il processo di gestione del rischio di violazione dei dati personali, derivante dal trattamento, secondo i principi della norma UNI ISO 31000 e realizzare una politica di sicurezza dei dati |

| | |
|---|---|
| | personali partecipata e condivisa con gli interessati e gli stakeholder. |
| | **OBIETTIVO OPERATIVO N. 4**<br>Garantire la correlazione con il PTPC e gli altri strumenti di pianificazione, mediante inserimento degli obiettivi strategici in tema di protezione dei dati personali nei documenti di pianificazione del titolare. |

Letto, approvato e sottoscritto:

| Il Vicesindaco | Il Segretario Comunale |
|---|---|
| F.to CASTELLANI EDI | F.to PERRONI BENEDETTO |

**PARERI DI CUI ALL'ARTICOLO 49, COMMA 1, D.LGS. N. 267/2000**

In merito alla REGOLARITA' TECNICA esprime, per quanto di competenza, parere Favorevole

Treia, lì 01-09-2018

IL RESPONSABILE DEL SERVIZIO
F.to PERRONI BENEDETTO

---

Si certifica che la presente deliberazione:

- viene pubblicata nel sito web istituzionale di questo Comune dal 30-10-2018 al 14-11-2018 (articolo 32, comma 1, della legge 18/06/2009, n. 69);
- Viene contemporaneamente comunicata, in elenco, ai capigruppo consiliari con lettera protocollo n. ai sensi dell'articolo 125, comma 1, del D.Lgs. 18/08/2000, n. 267.

Treia, lì 30-10-2018

IL SEGRETARIO COMUNALE
F.to PERRONI BENEDETTO

---

Copia conforme all'originale per uso amministrativo.

Treia, lì 30-10-2018

IL SEGRETARIO COMUNALE
PERRONI BENEDETTO

---

La presente deliberazione è divenuta esecutiva il giorno _____:

- ☐ in quanto dichiarata immediatamente eseguibile (articolo 134, comma 4, del D.Lgs. n. 267/2000);
- ☐ decorsi 10 giorni dalla pubblicazione (articolo 134, comma 3, del D.Lgs. n. 267/2000);
- ☐ decorsi 15 giorni dalla pubblicazione (articolo 9 dello statuto comunale).

Treia, lì _____

IL SEGRETARIO COMUNALE
F.to PERRONI BENEDETTO

---

Copia conforme all'originale per uso amministrativo.

Treia, lì_____

IL SEGRETARIO COMUNALE
PERRONI BENEDETTO

---

Assegnata al Settore:

| 1 | 2 | 3 | 4 | 5 | 6 | Segr. |
|---|---|---|---|---|---|---|