COPIA

Deliberazione n° 16 in data 21/02/2019

COMUNE DI FABBRICO

PROVINCIA DI REGGIO EMILIA

Verbale di Deliberazione di Giunta Comunale

Oggetto: DEFINIZIONE DEGLI OBIETTIVI STRATEGICI IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI.

L'anno 2019, addì 21 del mese di Febbraio alle ore 15:30 in FABBRICO, in seguito a regolari inviti si è riunita la GIUNTA COMUNALE presso la sala delle adunanze.

Eseguito l'appello, risultano:

			Presenze
1	TERZI MAURIZIO	Sindaco	S
2	DEGOLA ANDRADE CUNHA FABRIZIO	Vice Sindaco	N
3	NEGRI CRISTINA	Assessore	S
4	SCARDOVELLI PATRIZIA	Assessore	S
5	VIONI DARIO	Assessore	S
	TOTALE PRESENTI		4
	TOTALE ASSENTI		1

Assiste alla seduta il SEGRETARIO del Comune Dott. PASQUALE SCHIANO.
Il Sig. TERZI MAURIZIO nella sua qualità di Sindaco assume la presidenza e, riconosciuta legale l'adunanza dichiara aperta la seduta, ed invita l'assemblea a discutere e deliberare sull'oggetto sopraindicato.

GC16/2019

Definizione degli obiettivi strategici in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali.

LA GIUNTA COMUNALE

Premesso 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;
- 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;
- 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");
- che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale divenuto definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;
- 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;
- la Legge 25 ottobre 2017, n. 163 e, in particolare, l'art. 13, ha delegato il Governo per l'adeguamento della normativa nazionale alle disposizioni del GDPR (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;
- successivamente è stato adottato il D.Lgs. 10 agosto 2018 n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 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 (regolamento generale sulla protezione dei dati)", entrato in vigore il 19 settembre 2018;

Preso 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, 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.

j) *La gestione del rischio è dinamica*. La gestione del rischio è sensibile e risponde al cambiamento continuamente. Ogni qual volta 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.

k) *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 sono state attuate;

Ritenuto, pertanto, di includere, negli obiettivi strategici che il titolare intende perseguire per l'anno 2019 anche l'adozione di un apposito Piano di protezione dei dati personali e di gestione del rischio di violazione;

Richiamato:

- la deliberazione della Giunta comunale n. 55 del 17 maggio 2018 con la quale si è disposto di esternalizzare il servizio di adeguamento al Regolamento UE 679/2016 e il servizio di Responsabile della protezione dei dati personali non rilevando all'interno dell'Ente figure in grado di svolgere autonomamente le attività previste dal GDPR delegando l'Unione dei comuni Pianura Reggiana la procedura di affidamento a soggetto esterno di tale servizio;
- l'atto di designazione di designazione del Presidente dell'Unione dei comuni Pianura Reggiana in data 7 novembre 2018 che individua l'Avv. Nadia Corà, con sede a Volta Mantovana (Mn) in Via San Martino 8/b quale Responsabile della protezione dei dati personali) RPD per l'Unione dei Comuni Pianura Reggiana e per i comuni di Campagnola Emilia, Correggio, Fabbrico, Rio Saliceto, Rolo e San Martino in Rio, in forza di stipulazione di contratto di servizio con la persona giuridica ICAR S.r.l. con sede a Reggio Emilia

Dato atto che nella definizione degli obiettivi strategici di cui alla presente deliberazione si è tenuto conto delle indicazioni fornite dal Responsabile della protezione dei dati personali incaricato;

Preso atto dell'allegato parere favorevole, espresso sulla presente deliberazione da Responsabile dell'area amministrativa, ai sensi degli artt. 49 e 147bis comma 1 del D.Lgs. 267/200, in ordine alla regolarità tecnica, attestante la regolarità e la correttezza dell'azione amministrativa;

Con voti unanimi, resi nei modi di legge;

DELIBERA

1) Di definire, come di seguito riportati e in ragione di quanto sopra premesso, per l'anno 2019 i seguenti obiettivi strategici dell'intestato titolare in materia di protezione dei dati personali con riguardo al trattamento, al fine del loro recepimento e conseguente declinazione nei vari documenti di programmazione strategico-gestionale del titolare:

OBIETTIVI STRATEGICI
OBIETTIVO n. 1 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 n. 2 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 n. 3 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 n. 4 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.

2) Di disporre che il presente provvedimento sia pubblicato sul sito istituzionale dell'Ente nella sezione "Amministrazione trasparente" - "Disposizioni generali" - "Atti generali";

3) 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.

Deliberazione di Giunta n. 16 del 21/02/2019

Letto approvato e sottoscritto

PRESIDENTE
TERZI MAURIZIO

IL SEGRETARIO COMUNALE
Dott. PASQUALE SCHIANO

DICHIARAZIONE DI IMMEDIATA ESEGUIBILITA' (ART. 134 COMMA 4 D.LGS. 267/2000)

La presente deliberazione: /X/ è stata resa /__/ non è stata resa immediatamente eseguibile il giorno 21 febbraio 2019, ai sensi dell'art. 134 comma 4 del D.Lgs. 267/2000.

IL SEGRETARIO COMUNALE
Dott. PASQUALE SCHIANO

CERTIFICATO DI PUBBLICAZIONE E COMUNICAZIONE AI CAPIGRUPPO CONSILIARI (ARTT. 124 e 125 D.LGS. 267/2000)

- Copia della presente deliberazione viene :

Pubblicata mediante affissione all'Albo Pretorio del Comune, ai sensi dell'art. 124 D.Lgs. 18.08.2000 n. 267 da oggi

_____ per 15 giorni consecutivi

Comunicata contestualmente ai capigruppo consiliari, ai sensi dell'art.125 D.Lgs. 18.08.2000 n. 267 con nota prot. n.

_____ del _____ .

IL SEGRETARIO COMUNALE
Dott. PASQUALE SCHIANO

IL SEGRETARIO COMUNALE

CERTIFICATO DI ESECUTIVITA' (ART. 134 COMMA 3 D.LGS. 267/2000)

Si certifica che la presente deliberazione è divenuta **ESECUTIVA** il _____ per decorrenza dei dieci giorni dalla data di inizio della pubblicazione non avendo ricevuto richieste scritte e motivate con l'indicazione di norme violate, ai sensi degli artt. 127 e 134 del D.Lgs. 267/2000.

Addì

IL SEGRETARIO COMUNALE
Dott. PASQUALE SCHIANO

IL SEGRETARIO COMUNALE