COMUNE DI ASSAGO

Città Metropolitana di Milano

DELIBERAZIONE DI GIUNTA

Nº. 86 del 22-07-2019

Oggetto: Approvazione del registro dei trattamenti di cui all'art. 30 del GDPR UE 2016/679

L'anno duemiladiciannove il giorno ventidue del mese di luglio alle ore 14:30, nella Residenza Municipale, previa l'osservanza di tutte le formalità prescritte dalla legislazione vigente, è stata convocata la Giunta comunale.
Per l'assunzione di questo atto risultano:

COGNOME E NOME	CARICA	Presente Assente
Lara Carano	**SINDACO**	Presente
Mario Burgazzi	**ASSESSORE**	Presente
Marco La Rosa	**ASSESSORE**	Presente
Donatella Santagostino	**ASSESSORE**	Presente
Rosaria Incarbone	**ASSESSORE**	Assente

SINDACO E ASSESSORI ASSEGNATI n° 5

Presenti con diritto di voto nº. 4

Partecipa alla seduta il Dott. Salvatore Pagano, in qualità di Segretario Generale.
Lara Carano assume la presidenza e, riconosciuta legale l'adunanza dichiara aperta la seduta.

RICHIAMATO il Codice dell'Amministrazione Digitale, D.Lgs. n. 82/2005, così come modificato dal D.Lgs. n. 179/2016, che all'art. 51, rubricato "Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni", prevede che "i documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta";

PRESO ATTO che con Circolare del 18 aprile 2017, n. 2/2017, pubblicata in G.U. Serie Generale n. 103 del 5.05.2017, l'Agenzia per l'Italia Digitale (AGID), al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi delle Pubbliche Amministrazioni, ha disposto la sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" con nuove misure minime per la sicurezza informatica a cui le stesse Pubbliche Amministrazioni sono tenute a conformarsi entro il termine del 31.12.2017;

CONSIDERATO che il 25 maggio 2016 è entrato in vigore il Regolamento Europeo Privacy UE/2016/679 o GDPR (General Data Protection Regulation) che stabilisce le nuove norme in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali dati;

RILEVATO che il summenzionato Regolamento è direttamente applicabile in ciascuno degli Stati membri dell'Unione Europea ed entrerà in vigore il 25 maggio 2018;

CONSIDERATO che con il Regolamento Europeo Privacy UE/2016/679 viene recepito nel nostro ordinamento giuridico il "principio di accountability" (obbligo di responsabilizzazione) che impone alle Pubbliche Amministrazioni titolari del trattamento dei dati:

- di dimostrare di avere adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;

- che i trattamenti siano conformi ai principi e alle disposizioni del Regolamento, prevedendo, altresì, l'obbligo del titolare o del responsabile del trattamento della tenuta di apposito registro delle attività di trattamento, compresa la descrizione circa l'efficacia delle misure di sicurezza adottate;

- che il registro di cui al punto precedente, da tenersi in forma scritta o anche in formato elettronico, deve contenere una descrizione generale delle misure di sicurezza tecniche e organizzative e che su richiesta, il titolare del trattamento o il responsabile del trattamento sono tenuti a mettere il registro a disposizione dell'autorità di controllo;

TENUTO CONTO, inoltre, che il Regolamento Europeo Privacy UE/2016/679 ha:

- disciplinato la nuova figura del “Data Protection Officer” (DPO), responsabile della protezione dei dati personali che le Pubbliche Amministrazioni hanno l’obbligo di nominare al proprio interno e deve sempre essere “coinvolto in tutte le questioni riguardanti la protezione dei dati personali”;

- rafforzato i poteri delle Autorità Garanti nazionali ed inasprito le sanzioni amministrative a carico di imprese e Pubbliche Amministrazioni, in particolare, in caso di violazioni dei principi e disposizioni del Regolamento, le sanzioni possono arrivare fino a 10 milioni di euro o per le imprese fino al 2% - 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;

DATO ATTO che la nuova normativa europea fa carico alle Pubbliche Amministrazioni di non limitarsi alla semplice osservanza di un mero adempimento formale in materia di privacy, conservazione e sicurezza dei dati personali, ma attua un profondo mutamento culturale e concettuale con un rilevante impatto organizzativo da parte dell'Ente nell'ottica di adeguare le norme di protezione dei dati ai cambiamenti determinati dalla continua evoluzione delle tecnologie (cloud computing, digitalizzazione, social media, cooperazione applicativa, interconnessione di banche dati, pubblicazione automatizzata di dati on line) nelle Amministrazioni Pubbliche;

RITENUTO, pertanto, necessario realizzare un "modello organizzativo" da implementare in base ad una preliminare analisi dei rischi e ad un'autovalutazione finalizzata all'adozione delle migliori strategie volte a presidiare i trattamenti di dati effettuati, abbandonando l'approccio meramente formale del D.Lgs. 196/2003, limitato alla mera adozione di una lista "minima" di misure di sicurezza, realizzando, piuttosto, un sistema organizzativo caratterizzato da un'attenzione multidisciplinare alle specificità della struttura e della tipologia di trattamento, sia dal punto di vista della sicurezza informatica e in conformità agli obblighi legali, sia in considerazione del modello di archiviazione e gestione dei dati trattati. Tutto questo prevedendo, al contempo, non solo l'introduzione di nuove figure soggettive e professionali che dovranno presidiare i processi organizzativi interni per garantire un corretto trattamento dei dati personali, tra cui la figura del Responsabile della Protezione dei dati personali (DPO), ma altresì l'adozione di nuove misure tecniche ed organizzative volte a garantire l'integrità e la riservatezza dei dati, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la verifica e la valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento ;

VISTA la necessità di ottemperare agli obblighi imposti dal Regolamento Europeo Privacy UE/2016/679 o GDPR (General Data Protection Regulation) che stabilisce le nuove norme in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali dati;

RITENUTO di avviare il percorso di accountability, disponendo l'implementazione del software di gestione del registro trattamenti messo a disposizione da RobyOne srl, ai sensi dell'art.30 del GDPR UE 2016/679 e di approvare il documento allegato, che costituisce parte integrante e sostanziale del presente atto;

Visto l’art. 48, decreto legislativo 267/2000;

Recepito il parere di regolarità tecnica di cui all’art. 49 del decreto legislativo 267/2000;

Con voti unanimi favorevoli resi in forma palese;

DELIBERA

1. Di riconoscere quale Titolare del trattamento dei dati il Comune di Assago;

2. Di individuare quale rappresentante del Titolare del trattamento dei dati il Sindaco pro Tempore;
3. Di prendere atto che, ai sensi del GDPR UE 2016/679, sono stati nominati responsabili del trattamento dati tutti i Responsabili di Area del Comune di Assago;

4. Di individuare quali Responsabili esterni al trattamento dei dati personali tutti i soggetti, fisici o giuridici, che sono entrati o entreranno in possesso di banche dati contenenti dati personali in virtù di rapporti contrattuali con il Comune di Assago, individuando tutti i soggetti che saranno richiamati all'interno del registro dei trattamenti. A tali soggetti saranno comunicate apposite istruzioni in materia di trattamento dei dati forniti dal Comune di Assago;

5. Di prendere atto che il DPO è la dott.ssa Anita Macente con contratto di servizio con l'azienda Robyone srl Via Lazzaretto, 10B - 35010 Trebaseleghe (PD);

6. Di prendere atto che sono stati comunicati il nominativo ed i contatti del Responsabile della Protezione dei Dati al Garante per la Protezione dei Dati Personali;

7. Di prendere atto che il nominativo ed i contatti del Responsabile della Protezione dei Dati, nonché tutti gli atti riguardanti la tutela dei dati personali sono resi disponibili in apposita sezione in home page del sito istituzionale del Comune di Assago;

8. Di disporre, quale strumento primario per l'avvio di un percorso di accountability, il registro dei trattamenti messo a disposizione da RobyOne srl, da redigere con tutte le informazioni richieste dall'art.30 del GDPR UE 2016/679;

9. Di approvare il registro dei trattamenti allegato;

10. Di dare atto che è stato avviato un percorso di compliance normativa al GPDR UE 2016/679, anche attraverso la collaborazione del Responsabile della Protezione dei Dati, che si concretizza nelle seguenti attività:
- revisione ed aggiornamento della modulistica in dotazione al Comune di Assago: modelli di informativa e template di raccolta dei dati, ai sensi degli artt. 12-13-14 del GDPR UE 2016/679;
- verifica ed implementazione delle misure fisiche, ai sensi del GDPR UE 2016/679, a tutela della riservatezza dei dati personali, conservati in forma cartacea ed elettronica, di cui il Comune di Assago è titolare del trattamento;
- verifica ed implementazione delle misure tecniche ed informatiche, ai sensi del GDPR UE 2016/679, a tutela della riservatezza dei dati personali, conservati in forma cartacea ed elettronica, di cui il Comune di Assago è titolare del trattamento (sala server, accesso al server, log degli accessi e delle operazioni, controllo postazioni computer, sistemi operativi, antivirus, policy delle password, firewall, antivirus, policy della posta elettronica, policy dell'estrazione dei dati su dispositivi di massa e di memorizzazione dati);
- approvazione, ai sensi dell'art. 33 del GDPR UE 2016/679, con successiva deliberazione, del registro delle violazioni dei dati personali e della procedura di data breach nonché adeguamento del Codice di comportamento dei dipendenti del Comune di Assago al rispetto delle regole in materia di trattamento dai personali;

11. Di prendere atto che sono stati progettati percorsi formativi generali e puntuali rivolti ai dipendenti dell'ente, ai designati al trattamento dei dati personali, al Titolare e ai Responsabili del trattamento;
12. Di assegnare al Responsabile della Protezione dei Dati individuato il compito di aggiornare periodicamente, attraverso l'invio di articoli di approfondimento e/o link a webinar gratuiti, il Titolare del trattamento ed i designati al trattamento dei dati sulle novità normative in materia di protezione e trattamento dei dati personali;

13. Di ritenere disapplicata ed assorbita ogni regolamentazione contraria del Comune di Assago rispetto alle previsioni del GDPR UE 2016/679;

14. Di pubblicare il presente atto nell'apposita Sezione del sito internet comunale.

Il presente verbale viene letto e sottoscritto come segue:

Firmato digitalmente Il SINDACO Lara Carano	Firmato digitalmente Il Segretario Generale Dott. Salvatore Pagano