



**COMUNE
DI
MIRANDOLA**
Provincia di Modena

DELIBERAZIONE DELLA GIUNTA COMUNALE

N. 193

Del **21/10/2019**

Oggetto:

Adempimenti in attuazione al Regolamento UE 2016/679 (General Data Protection Regulation - GDPR). Approvazione Registro delle Attività di Trattamento, informative complete ed essenziali, disposizioni procedurali in materia di incidenti di sicurezza e violazioni di dati personali e adozione del relativo Registro "Data Breach".

L'anno **duemiladiciannove**, questo giorno **ventuno** del mese di **ottobre** alle ore 15,30 nella nuova sede comunale di via G. Giolitti n. 22, appositamente convocata, si è riunita la Giunta Comunale.

Fatto l'appello, sono presenti i Sigg.ri:

1) GRECO	ALBERTO	SINDACO	Si
2) BUDRI	LETIZIA	VICESINDACO	Si
3) CANOSSA	ANTONELLA	ASSESSORE	Si
4) FORTE	GIUSEPPE	ASSESSORE	Si
5) GANDOLFI	FABRIZIO	ASSESSORE	Si
6) MARCHI	MARINA	ASSESSORE	No

Presenti: **5**

Partecipa il Segretario Generale avv. MANCO MARIA ASSUNTA

Essendo legale il numero degli intervenuti, il Sig. GRECO ALBERTO SINDACO assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

Al termine della trattazione dell'argomento iscritto col n.2 all'ordine del giorno, si da atto che è presente l'Assessore Marina Marchi ed è assente l'Assessore Antonella Canossa.
Sono presenti, pertanto, il Sindaco e n.4 Assessori

Il Sindaco Alberto Greco illustra la proposta di deliberazione n. 14806, avente ad oggetto "Adempimenti in attuazione al Regolamento UE 2016/679 (General Data Protection Regulation - GDPR). Approvazione Registro delle Attività di Trattamento, informative complete ed essenziali, disposizioni procedurali in materia di incidenti di sicurezza e violazioni di dati personali e adozione del relativo Registro "Data Breach".";

Visti:

- lo schema di proposta predisposto dal Responsabile del Procedimento, dott.ssa Alice Incerti, allegato al presente atto per farne parte integrante e sostanziale, sotto la lettera "A";
- l'allegato parere di regolarità tecnica espresso dal Responsabile del Servizio Segreteria, Protocollo e Archivio, incaricato di posizione organizzativa, dott.ssa Alice Incerti, ai sensi dell'art. 49 - comma 1° - del D.Lgs. 18.8.00 n. 267 (Allegato "A");
- l'allegato parere di regolarità contabile espresso dal Responsabile del Servizio Finanziario, incaricato di posizione organizzativa, dott.ssa Katia Di Eleuterio (atto prot. n.37801 del 30-09-2019), ai sensi dell'art. 49, comma 1, del D. Lgs. n. 267 del 18 Agosto 2000 (Allegato "B");

Il Sindaco Alberto Greco pone, quindi, in votazione la proposta di deliberazione;

LA GIUNTA COMUNALE

Con voto unanime, reso per alzata di mano, proclamato dal Presidente;

D E L I B E R A

di approvare la proposta di deliberazione n. 14806, avente ad oggetto "Adempimenti in attuazione al Regolamento UE 2016/679 (General Data Protection Regulation - GDPR). Approvazione Registro delle Attività di Trattamento, informative complete ed essenziali, disposizioni procedurali in materia di incidenti di sicurezza e violazioni di dati personali e adozione del relativo Registro "Data Breach".", allegata al presente atto per farne parte integrante e sostanziale, sotto la lettera "A" e relativi allegati.

Con voto unanime, reso per alzata di mano, proclamato dal Presidente, delibera altresì di dichiarare, ai sensi dell'art. 134, comma 4, del D. Lgs. n. 267 del 18 Agosto 2000, immediatamente eseguibile il presente atto, al fine di consentire l'attuazione del percorso di *accountability* e *compliance* normativa dell'Ente ai dettami imposti dal Regolamento UE 2016/679.

SERVIZIO SEGRETERIA PROTOCOLLO E ARCHIVIO

Alla Giunta Comunale

Oggetto:

Adempimenti in attuazione al Regolamento UE 2016/679 (General Data Protection Regulation - GDPR). Approvazione Registro delle Attività di Trattamento, informative complete ed essenziali, disposizioni procedurali in materia di incidenti di sicurezza e violazioni di dati personali e adozione del relativo Registro "Data Breach".

Dato atto che il 4 maggio 2016 è stato pubblicato in Gazzetta Ufficiale Europea il Regolamento Europeo Privacy 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, e che abroga le direttive 95/46/CE (Regolamento generale sulla protezione dei dati);

Rilevato che il summenzionato Regolamento è entrato in vigore ed è direttamente applicabile in ciascuno degli Stati membri dell'Unione Europea a partire dal 25 maggio 2018;

Constatato che con il Regolamento UE 2016/679 viene recepito nel nostro ordinamento giuridico il "principio di accountability" (principio di responsabilizzazione) che impone alle Pubbliche Amministrazioni, in qualità di titolari del trattamento dei dati:

- di dimostrare di avere adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza opportuno 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 un "Registro delle Attività di Trattamento" svolte sotto la propria responsabilità, comprensivo delle informazioni di cui all'art. 30, commi 1 e 2 del Regolamento UE 2016/679, nonché della descrizione circa l'efficacia delle misure di sicurezza adottate;

- che, sulla base del disposto dell'art. 30, commi 3 e 4, del Regolamento UE 2016/679, 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 o il responsabile del trattamento sono tenuti a mettere il registro a disposizione dell'autorità di controllo;

- che, ai sensi dell'art. 13 del Regolamento UE 2016/679, in caso di raccolta dati dell'interessato, il titolare del trattamento è tenuto a fornirgli molteplici informazioni quali l'identità ed i dati di contatto del titolare (lettera a), i dati di contatto del R.P.D. (lettera b), le finalità del trattamento cui sono destinati i dati particolari nonché la base giuridica del trattamento (lettera c), gli interessi legittimi perseguiti dal titolare (lettera d), eventuali destinatari dei dati personale (lettera e), l'intenzione di trasferire i dati acquisiti in un paese terzo (lettera f); ed inoltre, in ossequio al comma 2, del medesimo art. 13, il periodo di conservazione (lettera a), l'esistenza del diritto d'accesso (lettera b), l'esistenza del diritto di revoca del consenso (lettera c), il diritto di reclamo (lettera d), le

conseguenze della mancata comunicazione dei dati (lettera e), l'esistenza di un processo decisionale automatizzato (lettera f);

Accertato inoltre come, tra gli adempimenti sopra prescritti, rientrano quelli previsti dal disposto dettato dagli artt. 33 e 34 del Regolamento UE 2016/679, specificatamente relativi al tema della notifiche e comunicazioni all'autorità di controllo in caso di violazione di dati personali, implicando conseguentemente per l'Ente l'onere di adottare una procedura ad hoc disciplinante la gestione delle violazioni di dati personali ("data breach") e la correlata istituzione di un apposito registro (Registro Data Breach) all'interno del quale documentarvi le informazioni relative a qualsiasi violazione di dati personali ed i provvedimenti adottati per porvi rimedio, al fine di consentire all'autorità di controllo, qualora si verificassero i presupposti, di verificare il rispetto della normativa;

Tenuto conto, altresì:

- che il Regolamento UE 2016/679 ha disciplinato la nuova figura del Responsabile della Protezione dei dati personali che le Pubbliche Amministrazioni hanno l'obbligo di designare al loro interno, se dipendente del titolare del trattamento, oppure con un contratto di servizio, e che deve sempre essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, come da disposto art. 38 del suddetto Regolamento;

- che è stata stipulata, ai sensi dell'art. 30 del D. Lgs. 267/2000, la convenzione per l'espletamento in forma associata di una procedura di gara per l'individuazione del contraente per l'affidamento dei servizi di adeguamento alla normativa contenuta nel Regolamento UE 2016/679 e per il conferimento dell'incarico di Responsabile della Protezione dei dati personali per l'Unione Comuni Modenesi Area Nord e gli Enti aderenti, fra cui il Comune di Mirandola, e associati;

- che con determinazione dirigenziale U.C.M.A.N. n. 418 del 13/07/2018, al fine di adempiere all'attuazione dei dettami previsti dal Regolamento UE/2016/679 e, nello specifico, dall'art. 73 cc. 1 e 2 del Codice dell'Amministrazione Digitale (CAD) che definisce e disciplina il sistema pubblico di connettività e cooperazione, si è proceduto ad affidare la fornitura dei Servizi di Cloud Computing – SPC per la gestione dei servizi professionali di sicurezza, all'operatore economico Telecom Italia S.p.A. nell'ambito dell'accordo quadro sottoscritto da Consip S.p.A.;

- che con atto - prot. n. 29817 del 20 settembre u.s., a seguito di espletamento di procedura negoziata con RdO (Richiesta di Offerta) su MEPA in esecutività della determinazione dirigenziale UCMAN n. 393 del 05/07/2018, il Sindaco nella sua qualità di Titolare del Trattamento ha designato quale Responsabile della Protezione dei dati personali (RPD), ai sensi dell'art. 37 del Regolamento UE 2016/679, lo Studio di Commercialisti "Bisi" di Modena, che ha indicato quale referente per lo svolgimento delle suddette funzioni il dott. Francesco Riso;

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 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 nelle amministrazioni pubbliche;

Ritenuto, dunque, opportuno:

- implementare un modello organizzativo basato sulla preliminare analisi dei rischi ed autovalutazione, finalizzate all'adozione delle migliori strategie volte a presidiare i trattamenti di dati effettuati, realizzando un sistema organizzativo caratterizzato da un'attenzione

multidisciplinare alle specificità della struttura dell'Ente e alla tipologia dei trattamenti effettuati, sia dal punto di vista della sicurezza informatica ed in conformità agli obblighi legali, sia in considerazione del modello di archiviazione e gestione dei dati trattati;

- prevedere, al contempo, non solo l'introduzione di una serie di figure soggettive e professionali che dovranno presidiare i processi organizzativi interni per garantire un corretto trattamento dei dati personali, tra cui la soprarichiamata figura del Responsabile della Protezione dei dati personali (RPD), ma altresì l'adozione di nuove misure tecniche ed organizzative volte ad assicurare l'integrità e la riservatezza dei dati, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico, nonché la verifica e la valutazione dell'efficacia delle misure tecniche e organizzative adottate al fine di garantire un adeguato livello di sicurezza del trattamento a fronte del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;

Ravvisato che, sulla base di quanto sopra esposto, in un'ottica di *accountability*, il Comune di Mirandola è tenuta all'adozione di un Registro delle Attività di Trattamento svolte sotto la propria responsabilità, in ottemperanza a quanto stabilito dall'art. 30 comma 1 del Regolamento UE 2016/679, documento che ha il fine di:

- consuntivare e storicizzare i trattamenti di dati personali effettuati dall'Ente nonché ogni altra attività relativa alla gestione delle informazioni connesse al perseguimento dei fini istituzionali;

- fornire all'Ente, ai suoi dipendenti, alle eventuali risorse in distacco e anche ai consulenti esterni, istruzioni organizzative e tecniche che consentano l'osservanza degli obblighi e, quindi, il rispetto delle prescrizioni previste dall'attuale normativa in materia di protezione dei dati personali;

- delineare il quadro di sicurezza del sistema informativo e di affidabilità dei relativi programmi informatici ai fini della tutela dei dati personali trattati;

- avere piena coscienza del grado di esposizione del proprio patrimonio informativo ai rischi specifici come individuati dalla normativa in materia di protezione del dato personale, in modo da poter applicare le misure per la sicurezza dei dati trattati soprattutto attraverso gli strumenti elettronici;

- dimostrare il percorso di adeguamento effettuato per garantire la compliance al Regolamento UE 2016/679;

Acquisiti:

- con nota del 7/08/2019, agli atti del protocollo generale col n. 25050/2019, il Registro delle categorie di attività di trattamento del Comune di Mirandola, Allegato 1 al presente atto a formarne parte integrante e sostanziale, elaborato dalla società Colin & Partners – Consulente Legale Informatico, in forza del contratto in essere con l'operatore economico Telecom Italia S.p.A. nell'ambito dell'Accordo Quadro CONSIP S.p.A., in esecuzione della determinazione sopraccitata n. 418/2018:

- con nota agli atti del protocollo generale col n. 31372/2019, le informative complete ed essenziali, Allegato 4 al presente atto a formarne parte integrante e sostanziale, elaborate dalla società Colin & Partners – Consulente Legale Informatico, in forza del contratto in essere con l'operatore economico Telecom Italia S.p.A. nell'ambito dell'Accordo Quadro CONSIP S.p.A., in esecuzione della determinazione sopraccitata n. 418/2018, in particolare avuto riguardo alle

seguenti categorie di interessati: stagisti, volontari, visitatori, richiedenti impiego, fornitori, utenti, amministratori di sistema, amministratori, famigliari di utenti, dipendenti ed amministratori;

Valutata, altresì, l'esigenza di dettare precise disposizioni procedurali in caso di incidenti di sicurezza e di violazioni di dati personali ("data breach"), in attuazione del disposto degli artt. 33 e 34 del Regolamento UE 2016/679, attenendosi ad un'apposita procedura disciplinante la gestione delle violazioni suddette e di adottare il relativo Registro delle violazioni (Registro Data Breach) al fine di consentire all'autorità di controllo di verificare il rispetto della norma, nonché di definire le responsabilità dei diversi soggetti coinvolti nel processo di "Data Breach" qualora la violazione impatti su risorse informatiche e/o analogiche;

Visti, pertanto, i seguenti allegati al presente atto a formarne parte integrante e sostanziale:

- l'Allegato 2, contenente le linee guida procedurali disciplinanti la gestione delle violazioni di dati personali, elaborate dal suindicato Responsabile della Protezione dei dati personali (RPD) dott. Francesco Riso, acquisite agli atti del protocollo generale con n. 31267/2019;

- l'Allegato 3, contenente lo schema di Registro Data Breach pervenuto dalla sopracitata società Colin & Partners – Consulente Legale Informatico, acquisito agli atti del protocollo generale con n. 31263/2019;

Acquisito agli atti del prot. n. 32151 del 17 ottobre 2019 il parere favorevole rilasciato dal Responsabile della Protezione dei dati personali (RPD) dott. Francesco Riso, in merito alla verifica di conformità rispetto alla normativa vigente in materia di privacy della documentazione elaborata dalla società Colin & Partners – Consulente Legale Informatico relativamente all'Allegato 1 - Registro delle categorie di attività di trattamento del Comune di Mirandola, Allegato 3 - Schema di Registro Data Breach e Allegato 4 - Informative complete ed essenziali;

Richiamati i seguenti atti:

- il vigente Statuto dell'Unione;

- il D.Lgs. 18 agosto 2000 n. 267 ad oggetto "Testo Unico delle Leggi sull'Ordinamento degli Enti Locali" e ss.mm.ii;

- il D.Lgs. 196/2003 ad oggetto "Codice in materia di protezione dei dati personali" e ss.mm.ii;

- 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;

- il D.Lgs. 82/2005 "Codice dell'Amministrazione Digitale" e ss.mm.ii;

- il vigente Regolamento dell'Unione sull'ordinamento generale degli uffici e servizi;

Su proposta del responsabile del procedimento individuato nella persona della dott.ssa Alice Incerti, Responsabile del Servizio Segreteria, Protocollo, Archivio;

PROPONE DI DELIBERARE

- di approvare, quale strumento primario per l'avvio di un percorso di accountability in ottemperanza a quanto stabilito dal Regolamento UE 2016/679, il Registro delle Attività di Trattamento del Comune di Mirandola, Allegato 1 al presente atto a formarne parte integrante e sostanziale, elaborato dalla società Colin & Partners – Consulente Legale Informatico, in forza del contratto in essere con l'operatore economico Telecom Italia S.p.A. nell'ambito dell'Accordo Quadro CONSIP S.p.A., quale documento contenente le informazioni di cui all'art. 30, commi 1 e 2

- del Regolamento Europeo Privacy UE/2016/679, ancorché la mappatura storica delle operazioni di trattamento di dati personali svolte dall'Ente sotto la propria responsabilità;
- di approvare le informative complete ed essenziali, Allegato 4 al presente atto a formarne parte integrante e sostanziale, elaborate dalla società Colin & Partners – Consulente Legale Informatico, in forza del contratto in essere con l'operatore economico Telecom Italia S.p.A. nell'ambito dell'Accordo Quadro CONSIP S.p.A., in esecuzione della determinazione sopraccitata n. 418/2018, in particolare avuto riguardo alle seguenti categorie di interessati: stagisti, volontari, visitatori, richiedenti impiego, fornitori, utenti, amministratori di sistema, amministratori, famigliari di utenti, dipendenti ed amministratori;
 - di approvare, altresì, in attuazione degli artt. 33 e 34 del Regolamento UE 2016/679, le linee guida procedurali disciplinanti la gestione delle violazioni di dati personali, elaborate dal Responsabile della Protezione dei dati (RPD) dott. Francesco Riso e il relativo schema di Registro "Data Breach" – rispettivamente Allegati 2 e 3 alla presente deliberazione a formarne parte integrante e sostanziale – al fine di consentire all'autorità di controllo di verificare il rispetto della norma, nonché di definire le responsabilità dei diversi soggetti coinvolti nel processo di "Data Breach" qualora la violazione impatti su risorse informatiche e/o analogiche;
 - di stabilire, in conformità a quanto disposto dal Regolamento UE 2016/679, che il Registro delle Attività di Trattamento di cui sopra, in funzione del carattere intrinseco di dinamicità che lo caratterizza per il censimento e l'analisi dei trattamenti effettuati dal Titolare, sia mantenuto costantemente aggiornato a fronte di qualsiasi cambiamento in ordine alle modalità, finalità, categorie di dati trattati e di interessati, affinché il contenuto dello stesso sempre corrisponda all'effettività dei trattamenti posti in essere dall'Ente, e di definire in via successiva gli aspetti legati alle disposizioni procedurali attinenti l'aggiornamento del registro in questione;
 - di demandare al Sindaco, nella sua qualità di Titolare del trattamento, tenuto conto della complessità della struttura e dell'impossibilità dello stesso di sovrintendere integralmente alla tutela ed alla gestione dei dati ed in considerazione della dislocazione logistica delle articolazioni interne dell'Ente, la nomina dei vari Responsabili del trattamento dei dati personali nonché la designazione del Referente della gestione delle violazioni dei dati personali nella persona del Dirigente del Settore Affari Generali, Promozione del Territorio e Sport, a cui affidare altresì la tenuta del Registro delle violazioni (Registro Data Breach), coadiuvato dalla figura del Responsabile della Protezione dei dati personali (RPD) dott. Francesco Riso in modo da garantire l'apporto professionale necessario alla corretta tenuta del registro in questione;
 - di addivenire, seguentemente all'approvazione della presente deliberazione, alla sottoscrizione digitale del Registro delle Attività di Trattamento da parte del Sindaco nella sua qualità di Titolare del trattamento;
 - di trasmettere la presente deliberazione al Responsabile della Protezione dei dati personali (RPD) e ai dirigenti e responsabili preposti ai vari settori e servizi dell'Ente che saranno designati Responsabili del trattamento dei dati personali;
 - di dare atto che il Registro delle Attività di Trattamento sia pubblicato sul sito istituzionale del Comune di Mirandola nella sezione "Amministrazione Trasparente";
 - di disporre che le informative sopraccitate siano rese, in prima istanza, all'interessato nella loro versione essenziale, tenendole comunque a disposizione nella loro versione completa, mediante pubblicazione sul sito istituzionale dell'Ente.

PROPONE DI DICHIARARE

ai sensi dell'art. 134, comma 4, del D. Lgs. n. 267 del 18 Agosto 2000, immediatamente eseguibile il presente atto, al fine di consentire l'attuazione del percorso di *accountability* e *compliance* normativa dell'Ente ai dettami imposti dal Regolamento UE 2016/679.

Il presente verbale viene letto e sottoscritto come segue:

IL PRESIDENTE
GRECO ALBERTO
F.to digitalmente

IL SEGRETARIO GENERALE
avv. MANCO MARIA ASSUNTA
F.to digitalmente

Ai sensi dell'art. 18, del d.P.R. n. 445/2000, e dell'art. 23 del C.A.D., io sottoscritto dipendente comunale, impiegato presso l'Ufficio di Segreteria generale, attesto che la presente copia, composta da n.__() facciate è conforme all'originale informatico, sottoscritto con firma digitale, conservato presso gli archivi digitali dell'Ente.

Mirandola,_____

Il funzionario addetto
