

DELIBERAZIONE DELLA GIUNTA COMUNALE

N.1 del registro Data 18/01/2024	REGOLAMENTO PRIVACY UE 2016/679 GENERAL DATA PROTECTION REGULATION (GDPR) APPROVAZIONE DEL REGISTRO DEI TRATTAMENTI EX ART. 30 GDPR E DEL REGISTRO DELLE VIOLAZIONI EX ART. 33 GDPR, INDIVIDUAZIONE FIGURE DELL'ORGANIGRAMMA PRIVACY, AGGIORNAMENTO DELLE ATTIVITÀ DI COMPLIANCE NORMATIVA AI SENSI DEL REGOLAMENTO UE RICHIAMATO.
-------------------------------------	---

L'anno duemilaventiquattro, il giorno diciotto del mese di Gennaio alle ore 17.30 e seguenti si è riunita nella sala delle adunanze del suddetto Comune, la Giunta Comunale con la presenza dei signori:

		Presenti	Assenti
Massimiliano Calcagni	Sindaco	P	
Atripaldi Ottavio	Vice Sindaco	P	
Carbone Luisa	Assessore	P	
Bottini Fabrizio	Assessore	P	
Colantonio Ivan	Assessore		X
Bianchini Manuela	Assessore		X

Partecipa con funzioni consultive, referenti e di assistenza e ne cura la verbalizzazione (art.97, c.4.a, del T.U. n. 267/2000), il Segretario Comunale Moreschini Marco.

Il Sindaco, dopo aver constatato che gli intervenuti sono in numero legale, dichiara aperta la riunione e invita i convocati a deliberare sull'oggetto sopra indicato.

LA GIUNTA COMUNALE

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;

Considerato che il 19 settembre 2018 è entrato in vigore il Decreto Legislativo 101/2018 recante la normativa di adeguamento italiana al Regolamento europeo privacy UE/2016/679;

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;

Ritenuto, quindi, opportuno implementare il Registro dei trattamenti, in modalità telematica, quale importante strumento di accountability, finalizzato a mappare in maniera puntuale i trattamenti dei dati personali concretamente effettuati dall'ente. Il Registro viene conservato digitalmente nel software in cloud messo a disposizione dell'ente da parte del DPO.

Ogni aggiornamento successivo che intervenga sul Registro, come previsto ai sensi dell'art. 30 del GDPR, (inclusa l'introduzione di nuove tecnologie o APP, portali web etc..) deve essere segnalata da parte dei vari soggetti Designati al trattamento al Responsabile per la protezione dei dati personali e al Responsabile organizzativo privacy dell'ente che verificheranno le modifiche introdotte segnalando eventuali adempimenti conseguenti.

Considerato che con la presente deliberazione doversi aggiornare il modello organizzativo come già approvato dalla deliberazione di Giunta Comunale n. 17 del 28.02.2019, adeguandolo alle modificazioni organizzative e legislative intercorse.

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;

Acquisito il parere di regolarità tecnica del Responsabile Organizzativo Privacy ai sensi degli art. 49 e 147-bis del d.lgs. 267 del 2000

DELIBERA

1. di riconoscere quale Titolare del trattamento dei dati il Comune di Rocca di Papa rappresentato dal Sindaco pro-tempore;
2. Di approvare il modello organizzativo che va ad adeguare e sostituire quello di cui alla delibera di Giunta Comunale numero 17 del 28.02.2019 secondo le seguenti disposizioni :
 - o individuare quali "designati al trattamento dei dati personali", ai sensi del GDPR UE 2016/679 i Responsabili di Area all'uopo nominati del Comune di Rocca di Papa, che a loro volta individueranno i soggetti incaricati /autorizzati al trattamento dei dati all'interno dell'area di riferimento

- individuare il Segretario Generale quale Responsabile organizzativo Privacy del Comune di Rocca di Papa al quale vengono assegnate le seguenti funzioni:
 - coordinatore generale in materia di trattamento dei dati personali e tutela della riservatezza dei dati personali trattati dal Comune di Rocca di Papa;
 - coordinatore generale in materia di misure di sicurezza fisiche, tecniche ed organizzative a tutela della riservatezza dei dati personali trattati dal Comune di Rocca di Papa;
 - punto di riferimento per ogni eventuale comunicazione con il DPO esterno individuato e nominato;
 - individuare quali Responsabili del 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 Rocca di Papa individuando tutti i soggetti richiamati all'interno del registro dei trattamenti allegato alla presente. A tali soggetti saranno comunicate apposite istruzioni in materia di trattamento dei dati forniti dal Comune seguendo apposite nomine trasmesse a tutto il personale Designato.
2. di approvare la più recente versione del Registro dei Trattamenti del Comune, allegata alla presente (ALLEGATO A) ex art. 30 del GDPR che verrà aggiornato in via telematica tramite il Gestionale Idea Privacy in utilizzo da parte del Titolare e del Personale Designato con il Supporto del Nominato DPO;
 3. di verificare, con riguardo ai trattamenti di dati personali con maggiore esposizione a rischio per i diritti e le libertà delle persone fisiche interessate, Valutazioni di Impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 del GDPR UE 2016/679;
 4. di approvare, ai sensi dell'art. 33 del GDPR UE 2016/679, la più recente versione del registro delle violazioni dei dati personali che verrà aggiornato di volta in volta dal Responsabile Organizzativo Privacy (ALLEGATO B) di concerto con il DPO.
 5. di prendere atto che il Registro Accountability è un file dinamico che verrà aggiornato e protocollato periodicamente da parte del Responsabile Organizzativo Privacy di concerto con il DPO, quale strumento indispensabile a dimostrare il compimento di tutte le attività espletate e da effettuare volte all'adempimento del modello organizzativo del Comune di Rocca di Papa in ambito protezione dei dati personali, quali a titolo esemplificativo: incontri formativi, incontri informativi, politiche di sensibilizzazione, impostazione del registro delle attività di trattamento, completamento del registro delle attività di trattamento, impostazione del registro di accountability, aggiornamento del registro di accountability;
 6. di aggiornare tutti i soggetti coinvolti nella procedura e renderli partecipi di un percorso di compliance normativa rispetto al GDPR UE 2016/679, anche attraverso la consulenza del Responsabile della Protezione dei Dati, che si concretizzerà nelle seguenti attività:
 - revisione ed aggiornamento della modulistica in dotazione al Comune di Rocca di Papa 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 Rocca di Papa 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 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) attraverso l'adozione di una policy interna da diffondere al personale dipendente;

- progettazione di percorsi formativi/informativi generali e puntuali rivolti ai dipendenti dell'ente, ai designati al trattamento dei dati personali, al Titolare e ai Responsabili del trattamento;
- verifica dei principali adempimenti in materia di Videosorveglianza con particolare riguardo a: cartellonistica, informativa specifica e fornire parere su DPIA;
- adesione ad eventuali codici di condotta di cui all'art. 40 del GDPR UE 2016/679 al fine di limitare i potenziali rischi del trattamento per i diritti e le libertà delle persone fisiche;

Inoltre stante l'urgenza di rimanere conformi al dettato legislativo, con separata ed unanime votazione

DELIBERA

Di dichiarare la presene deliberazione immediatamente eseguibile ai sensi e per gli effetti dell'art. 134, comma 4 del d.lgs. 267 del 2000.



Estremi della Proposta

Proposta Nr. **2024 / 16**

Ufficio Proponente: **Atti Amministrativi**

Oggetto: **REGOLAMENTO PRIVACY UE 2016/679 GENERAL DATA PROTECTION REGULATION (GDPR) APPROVAZIONE DEL REGISTRO DEI TRATTAMENTI EX ART. 30 GDPR E DEL REGISTRO DELLE VIOLAZIONI EX ART. 33 GDPR, INDIVIDUAZIONE FIGURE DELL'ORGANIGRAMMA PRIVACY, AGGIORNAMENTO DELLE ATTIVITÀ DI COMPLIANCE NORMATIVA AI SENSI DEL REGOLAMENTO UE RICHIAMATO.**

Parere Tecnico

Ufficio Proponente (Atti Amministrativi)

In ordine alla regolarità tecnica della presente proposta, ai sensi dell'art. 49, comma 1, TUEL - D.Lgs. n. 267 del 18.08.2000, si esprime parere FAVOREVOLE.

Sintesi parere: **Parere Favorevole**

Data **18/01/2024**

Il Responsabile di Settore

Dott. Marco Moreschini

Il presente verbale viene così sottoscritto:

**IL SINDACO
MASSIMILIANO CALCAGNI**

**IL SEGRETARIO COMUNALE
MORESCHINI MARCO**

PUBBLICAZIONE ALL'ALBO

La presente deliberazione è pubblicata all'Albo per 15 giorni, ai sensi degli Artt. 124 e 134 del D.Lgs n. 267/2000 e dell'Art. 32 della Legge n. 69 del 18/06/2009

ESECUTIVITA'

Il Segretario attesta che la presente deliberazione è esecutiva

- è immediatamente eseguibile ai sensi dell'art. 134, comma 4 del D. Lgs. 267/2000
- È trasmessa ai capigruppo consiliari ai sensi dell'art. 125 del D. Lgs. 267/2000

Rocca di Papa, lì 22/01/24

**IL SEGRETARIO COMUNALE
MORESCHINI MARCO**

Il presente documento è sottoscritto con firma digitale - ai sensi degli art. 23, 25 DPR 445/2000 e art. 20 e 21 D.Lgs 82/2005 da:

Moreschini Marco in data 22/01/2024
Massimiliano Calcagni in data 23/01/2024

ATTESTAZIONE DI PUBBLICAZIONE ALL'ALBO

La presente deliberazione è pubblicata all'Albo per 15 giorni dal 23/01/2024 al 07/02/2024, ai sensi degli Artt. 124 e 134 del D.Lgs n.267/2000 e dell' Art. 32 della Legge n. 69 del 18/06/2009

Rocca di Papa, li 23/01/2024

Il Responsabile della Pubblicazione
Francesca Fondi

Il presente documento è sottoscritto con firma digitale - ai sensi degli art. 23, 25 DPR 445/2000 e art. 20 e 21 D.Lgs 82/2005 da:

FRANCESCA FONDI in data 23/01/2024