COMUNE DI MARANO SUL PANARO
Provincia di Modena

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Deliberazione n. 97 del 03/12/2018

OGGETTO: ADEGUAMENTO AL REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELL'UNIONE TERRE DI CASTELLI E NEI COMUNI ADERENTI

L'anno **duemiladiciotto** addì **tre** del mese di **dicembre** alle ore **17:30** nella Casa Comunale, previa l'osservanza di tutte le formalità prescritte dalla vigente legge comunale e provinciale, vennero oggi convocati a seduta i componenti la Giunta Comunale, che nelle persone seguenti risultano presenti alla trattazione della proposta di deliberazione in oggetto:

MURATORI EMILIA	SINDACO	Presente
GALLI GIOVANNI	VICE SINDACO	Presente
RONDELLI MAURO	ASSESSORE	Presente
DANI ELIO	ASSESSORE	Presente
ZANANTONI RITA	ASSESSORE	Presente

Presenti n. 5 **Assenti n. 0**

Partecipa il SEGRETARIO COMUNALE MARTINI MARGHERITA che provvede alla redazione del presente verbale.

Presiede la seduta, nella sua qualità di SINDACO, il Sig. MURATORI EMILIA che dichiara aperta la trattazione dell'oggetto sopra indicato.

Deliberazione n. 97 del 03/12/2018

OGGETTO: ADEGUAMENTO AL REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELL'UNIONE TERRE DI CASTELLI E NEI COMUNI ADERENTI

LA GIUNTA COMUNALE

PREMESSO che:

- il 25 maggio 2018 è entrato in vigore 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 (di seguito GDPR) il quale ha abrogato la direttiva 95/46/CE;
- il GDPR detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni;
- il GDPR individua inoltre diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti;
- il D.lgs. n. 196/2003 "*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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*", capo IV, art. 2 *quaterdecies*, come modificato dal D.lgs. 101/2018, stabilisce che il titolare del trattamento può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate che operano sotto la propria autorità e che il titolare del trattamento individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta;

RICHIAMATE le proprie precedenti deliberazioni:

- n. 98 del 20/12/2017 mediante la quale è stato nominato il Responsabile della transizione digitale nella persona della Dott.ssa Elisabetta Manzini e contestualmente sono stati individuati i contenuti dell'elenco delle Misure minime per la sicurezza ICT delle pubbliche Amministrazioni poi sottoscritti dal suddetto Responsabile entro il 31/12/2017 come prescritto dalla normativa in materia;
- n. 44 del 21/05/2018, con cui:
  - veniva designato quale Responsabile della Protezione dei Dati (RPD) del Comune di Marano sul Panaro la società Lepida S.p.A., con sede in Bologna – Via della Liberazione, 15 - 40128 Bologna;
  - veniva individuato quale Referente dell'Ente, incaricato di operare in qualità di coordinatore delle attività nei confronti dei soggetti interni e dialogare direttamente con il Responsabile della Protezione dei Dati (RPD), il Responsabile del Settore Amministrativo del Comune;
- n. 48 del 6/06/2018, con cui veniva adottato un modello organizzativo volto a presidiare il trattamento dei dati personali, dando atto del ruolo di supporto svolto dal Servizio "Sistemi Informativi" in collaborazione con il Referente dell'Ente nei confronti del RPD in tema di risorse strumentali e competenze e nel segnalare le eventuali violazioni dei dati ai fini della notifica al Garante;

RICHIAMATI inoltre:

- gli artt. 32 e 33 del GDPR che dispongono rispettivamente che devono essere approntate misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali e che in caso di violazione dei dati personali, il titolare deve notificare tale violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza;

- le "*Linee Guida sulla notifica delle violazioni dei dati personali ai sensi de regolamento (UE) 2016/679*", adottate il 3 ottobre 2017, poi emendate ed adottate in data 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione dei dati personali (cioè l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata) nelle quali vengono forniti dettagli sugli obblighi di notifica e di comunicazione delle violazioni sanciti dal GDPR, nonché alcune misure che i titolari del trattamento possono adottare per soddisfare i nuovi obblighi;

CONSIDERATO che in tema di sicurezza del trattamento dei dati personali il GDPR stabilisce che:

- le misure tecniche ed organizzative adottate dal Titolare del trattamento devono poter garantire un livello di sicurezza *adeguato* al rischio, tenuto conto di:
  - stato dell'arte e costi di attuazione;
  - natura, oggetto, contesto e finalità di trattamento;
  - rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- nella valutazione dei livelli di sicurezza occorre tener conto dei rischi del trattamento derivanti da: distruzione, perdita, modifica, divulgazione non autorizzata, accesso accidentale o illegale ai dati personali trasmessi, conservati o comunque trattati;
- nel caso di violazione di dati personali (c.d. *data breach*), il Titolare dovrà procedere alla sua notifica al Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui viene rilevata, previa valutazione dei rischi per i diritti e le libertà degli interessati;

DATO ATTO che la corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'Ente in caso di incidente; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti;

DATO ATTO inoltre 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" sulla base di una preliminare analisi dei rischi e di 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 di legge, sia in considerazione della gestione dei dati trattati. Tutto questo prevedendo, al contempo, non solo l'introduzione di nuove figure che dovranno presidiare i processi organizzativi interni per garantire un corretto trattamento dei dati personali, tra cui ad es. la figura del Responsabile della Protezione dei dati personali (RPD), 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 NECESSARIO quindi adottare uno specifico documento che, tenuto conto dell'organizzazione dell'Ente, disciplini all'interno del Comune l'uso dei sistemi informativi e fornisca indicazioni tecniche ed organizzative da applicare per garantire la sicurezza dei dati trattati con strumentazioni informatiche, nonché uno specifico documento che in caso di incidenti di sicurezza, informatica e non, che possono occorrere ai servizi e ai dati gestiti dal Comune, ne regolamenti la gestione;

TENUTO CONTO che la gestione dei servizi informativi è stata delegata all'Unione Terre di Castelli ma che l'interazione tra il Servizio Sistemi Informativi e i servizi/uffici dell'Ente è continua e costante;

VISTO l'allegato "Disciplinare per l'uso dei sistemi informativi nell'Unione Terre di Castelli e nei Comuni aderenti" (all. A) volto a fornire una disciplina sull'uso dei sistemi informativi che si propone anche lo scopo di impedire, o comunque ridurre, il rischio che eventuali problemi di sicurezza su una postazione o su un punto della rete si propaghino sfruttando l'interconnettività e l'interdipendenza fra le componenti del sistema informativo del Comune;

VISTO inoltre l'allegato modello di gestione degli incidenti di sicurezza (All. B) che oltre a prevedere la costituzione di una struttura operativa competente (c.d. "gruppo per la Gestione della Sicurezza ICT") in

grado di intervenire secondo le procedure operative prestabilite, individua, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016:

- le violazioni dei dati personali (c.d. *data breach*) che ricadono nell'ambito della normativa in materia di protezione dei dati, tenendo conto del fatto che tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni di dati personali;
- i casi in cui l'Ente deve notificare i *data breach* al Garante ed agli interessati;
- le misure atte a trattare il rischio e la documentazione da produrre;

VALUTATO che la struttura operativa deputata ad intervenire secondo le procedure operative prestabilite (c.d. "gruppo per la Gestione della Sicurezza ICT") debba essere costituita dalle seguenti figure:

- un dipendente del Servizio "Sistemi Informativi" dell'Unione;
- il Responsabile del Settore Amministrativo, già incaricato, con la richiamata deliberazione di Giunta n. 44 del 21.05.2018, quale referente nei rapporti con il RPD dell'Unione;
- il Responsabile del Settore nell'ambito del quale si è verificato la violazione;
- eventuali altri soggetti coinvolti nel trattamento dei dati oggetto di violazione che il gruppo riterrà necessario interessare a seconda della tipologia di incidente e della tipologia di dati coinvolti;

VISTO il parere reso dal RPD dell'Unione, prot. UNI n. 46097 del 9.11.2018, che ha confermato la coerenza del documento con i principi del GDPR;

RITENUTO, infine, in attuazione dell'art. 33, paragrafo 5, del GDPR (il quale prevede che il titolare del trattamento "*documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per provi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo*") ed in ossequio al principio di *accountability* come suggerito dalla Linee guida in materia adottate dal Gruppo di lavoro articolo 29 per la protezione dei dati, di istituire un registro interno delle violazioni in cui documentare tutte le violazioni, sia quelle notificabili che non notificabili, da tenere a cura del Responsabile del Settore Amministrativo, nella sua funzione di componente del Gruppo per la Gestione della sicurezza nonchè referente nei rapporti con il RPD dell'Unione;

VISTI:

- il D.Lgs. n. 267/2000;
- il GDPR 2016/679, ed in particolare gli artt. 32, 33 e 34 del Regolamento europeo;
- il D.Lgs. n. 196/2003, nel testo integrato con le modifiche introdotte dal D.Lgs. n. 101/2018;
- le "*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*", adottate il 3 ottobre 2017 ed emendate ed adottate in data 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione dei dati;
- lo Statuto Comunale;
- il vigente Regolamento degli uffici e dei Servizi;

VISTO il parere favorevole espresso ai sensi dell'art. 49, comma 1, e dell'art. 147 bis, comma 1, del D.Lgs. n. 267/2000 dal Responsabile del Settore Amministrativo in merito alla regolarità tecnica della proposta di deliberazione di cui sopra, parere allegato al presente atto quale parte integrante e sostanziale dello stesso;

DATO ATTO che ai sensi dell'art. 49, comma 1, del medesimo D.Lgs. n. 267/2000 il Responsabile del Settore Economico Finanziario non ha espresso alcun parere sulla regolarità contabile della proposta in oggetto in quanto la stessa è priva di rilevanza contabile e finanziaria;

Con voto unanime, favorevolmente espresso nei modi e forme di legge;

DELIBERA

1) Di approvare il "**Disciplinare per l'uso dei sistemi informativi nell'Unione Terre di Castelli e nei Comuni aderenti**", allegato al presente atto quale parte integrante e sostanziale (**all. A**), rivolto di impedire, o comunque ridurre, il rischio del verificarsi di problemi di sicurezza;
2) Di approvare, in attuazione degli adempimenti previsti dal Regolamento Europeo UE/2016/679, il "**Modello di gestione degli incidenti di sicurezza**", allegato al presente atto quale parte integrante e sostanziale (**all. B**) che definisce le procedure che il Comune di Marano sul Panaro adotta in caso di violazione dei dati personali;
3) Di disporre, contestualmente all'approvazione, l'immediata adozione da parte dell'Ente del suddetto modello che prevede, tra l'altro, la costituzione di una struttura operativa (c.d. "Gruppo per la Gestione della Sicurezza ICT") deputata ad intervenire in caso di incidente di sicurezza secondo le procedure operative prestabilite e costituita dalle seguenti figure:

- un dipendente del Servizio “Sistemi Informativi” dell'Unione;
- il Responsabile del Settore Amministrativo, già incaricato, con la richiamata deliberazione di Giunta n. 44 del 21.05.2018, quale referente nei rapporti con il RPD dell’Unione;
- il Responsabile del Settore nell’ambito del quale si è verificato la violazione;
- eventuali altri soggetti coinvolti nel trattamento dei dati oggetto di violazione che il gruppo riterrà necessario interessare a seconda della tipologia di incidente e della tipologia di dati coinvolti;

4) Di disporre, in attuazione dell’art. 33, paragrafo 5, del GDPR e delle “*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*” adottate dal Gruppo di lavoro articolo 29 per la protezione dei dati, in ossequi al principio di *accountability*, la tenuta di un apposito “**Registro delle violazioni di dati personali**” secondo il modello allegato (**all. C**) a cura del Responsabile del Settore Amministrativo;
5) Di pubblicare nella rete intranet dell’Ente, in apposita sezione, il presente atto, unitamente alla indicazione dei riferimenti di contatto del “Gruppo per la Gestione della Sicurezza ICT” nonché della procedura da attivare in caso di sospetta violazione di dati personali.

INDI

LA GIUNTA COMUNALE

Successivamente con votazione unanime e palese

stante l’urgenza di procedere per consentire il tempestivo adeguamento dell’Ente alle disposizioni del Regolamento Europeo UE/2016/679 in materia di sicurezza dei dati personali.

DELIBERA

- di rendere immediatamente eseguibile la presente deliberazione, ai sensi dell’art. 134, 4° comma del D.Lgs. 18 agosto 2000, n. 267

COMUNE DI MARANO SUL PANARO
Provincia di Modena

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

IL SINDACO	IL SEGRETARIO COMUNALE
MURATORI EMILIA	MARTINI MARGHERITA