COMUNE DI GARBAGNA
PROVINCIA DI ALESSANDRIA

COPIA

Codice ente	Protocollo n.
06079	0

DELIBERAZIONE N. 18
Soggetta invio capigruppo N☐
Trasmessa al C.R.C. ☐

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO: DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DI DATI PERSONALI

L'anno **duemilaventiquattro** addi **quattro** del mese di **aprile** alle ore 11.30, previa osservanza di tutte le formalita' prescritte dalla vigente legge, vennero oggi convocati a seduta, in modalità mista, ai sensi del regolamento comunale approvato dal consiglio comunale con delibera n. 18 del 28/07/2022, i componenti la Giunta Comunale. Al1'appello nominale, effettuato in modo telematico, risultano:

SEMINO FABIO	SINDACO	Presente
VERNA MAURIZIO	VICE SINDACO	Presente
MARUFFO JACOPO	ASSESSORE	Presente

Totale presenti 3
Totale assenti 0

Partecipa alla adunanza, dall'ufficio, il Segretario Comunale Dott. GIOVANNI OLIVOTTO il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti in video conferenza, il Sig. SEMINO FABIO nella sua qualita' di Sindaco assume la presidenza e dichiara aperta la seduta per la trattazione dell'argomento indicato in oggetto.

Comune di GARBAGNA

Provincia di Alessandria

ALLEGATO ALLA DELIBERA : G.C. n. 18 del 04.04.2024

OGGETTO : DISPOSIZIONI OPERATIVE IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DI DATI PERSONALI

Parere di regolarità tecnica.

Vista la suestesa proposta il sottoscritto esprime parere favorevole di regolarità tecnica, per quanto di competenza.

IL RESPONSABILE DEL SERVIZIO

F.to (Dott. Giovanni Olivotto)

Il Segretario Comunale attesta che la presente seduta di Giunta Comunale si è svolta in modalità mista, con i componenti Sig. Maruffo Jacopo e Sig. Verna Maurizio presenti in modalità telematica e il Sig. Semino Fabio in presenza

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;
- il Comune di Garbagna, in quanto Titolare del trattamento, è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (data breach), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati;

VISTO:
- 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 (Regolamento Generale sulla Protezione dei Dati, di seguito "Regolamento");
- il Decreto Legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal Decreto Legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 "Codice");
- il Decreto Legislativo 18 maggio 2018, n. 51, recante Attuazione della direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (di seguito "D.Lgs. n. 51/2018");
- le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" (WP250) del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato Europeo per la protezione dei dati il 25 maggio 2018;
- la Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adottata ai sensi dell'art. 64 del Regolamento, dal Comitato Europeo per la protezione dei dati in data 12 marzo 2019;
- il Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [doc-web n. 9126951];

CONSIDERATO CHE:
- in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare tale evento al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (artt. 33 e 55 del Regolamento, art. 2-bis del Codice);
- il titolare del trattamento è tenuto altresì a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni

giurisdizionali, nonché di quelle giudiziarie del Pubblico Ministero (artt. 26 e 37, comma 6, del D.Lgs. n. 51/2018);
- per «violazione dei dati personali» (data breach) si intende la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, punto 12 del Regolamento; art. 2, comma 1, lett. m, del D.Lgs. n. 51/2018);
- per la omessa notifica di data breach all'Autorità di controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, sono previste pesanti sanzioni amministrative (art. 83 GDPR), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui all'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- inoltre, l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile);
- lo stesso GDPR, all'art. 83 paragrafo 2, indica dei fattori che possono mitigare o aggravare la violazione e, tra questi, un elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del titolare che possa dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione.
L'atteggiamento reattivo e cooperativo comporta, inoltre, sicuramente un'attenuazione delle sanzioni applicabili;

RITENUTO PERTANTO:

a) di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (data breach policy). A tale riguardo si precisa che, presso il Titolare, sono già state attivate procedure a tutela della sicurezza dei dati, tra cui:
b) adottare le misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di incidente sulla sicurezza;
c) organizzare, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei dati personali e dei sistemi;
d) predisporre un sistema di protezione, mediante apposite misure tecniche (firewall, antivirus,…) dell'accesso a internet e ai dispositivi elettronici; b) strategico per l'ente:
e) sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);
f) definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
g) definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;
h) assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare tra le parti interessate;
i) stabilire che le procedure contemplate nell'approvando documento siano applicabili a tutte le attività svolte dal Titolare, con particolare riferimento alla gestione di tutti gli archivi e

documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati, anche con il supporto di fornitori esterni;

j) stabilire che il rispetto dell'adottanda procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia. In particolare le procedure medesime sono rivolte a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare, quali: i. I lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso del prestazioni richieste per conto del Titolare del trattamento; ii. qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare. In particolare, ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach;

VISTI il decreto con il quale è stato designato l'avv. Massimo Ramello quale Responsabile della Protezione dei Dati Personali (DPO), nel rispetto della vigente normativa;

VISTO il provvedimento di designazione del Referente, Canevaro Alessandra, al Responsabile della protezione dei dati personali e la deliberazione della Giunta Comunale n. 17 del 04 aprile 2024, con la quale è stato approvato il Piano di Protezione e modello organizzativo per la tutela dei dati personali;

VISTE le disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali (c.d. data breach)e loro allegati (lettere da A a D) e ritenute le stesse corrispondenti alla struttura organizzativa dell'Ente e adeguate sotto il profilo operativo alle esigenze del medesimo;

VALUTATA pertanto l'opportunità di procedere all'approvazione;

VISTI:
-il Regolamento sull'Ordinamento degli Uffici e dei Servizi;
-il D. Lgs. 267/2000 e s.m.i;
-Il D.Lgs. n. 165/2001 e s.m.i. Acquisito il preventivo parere favorevole sulla proposta della presente deliberazione, in ordine alla regolarità tecnica ai sensi dell'art. 49, commi 1, del D. Lgs. 267/00 e s.m.i. e dato atto che la presente deliberazione non comporta riflessi diretti o indiretti sulla situazione economicofinanziaria o sul patrimonio dell'Ente e pertanto, ai sensi del medesimo articolo, non necessita del parere di regolarità contabile;

Con voti favorevoli unanimi espressi in forma palese,

DELIBERA

1. di approvare, per le motivazioni in narrativa esposte che qui si intendono integralmente richiamate, la proceduta nel caso di violazione dei dati personali (data breach) del Comune di Garbagna, richiesta dagli articoli 33 e 34 del GDPR “Regolamento Generale sulla Protezione dei Dati” (Regolamento UE 2016/679) e relativi allegati da A) a D), che costituiscono parte integrante e sostanziale della presente deliberazione.

2. di demandare la concreta attuazione delle misure regolamentari minime contenute nelle disposizioni operative al personale operante all’interno dell’Ente nelle sue articolazioni gerarchiche e secondo le loro rispettive funzioni e competenze;

3. di inviare la procedura nel caso di violazione dei dati personali (data breach) del Comune di Garbagna al Responsabile del Trattamento dei Dati personali già nominato, in persona dell’Avv. Massimo Ramello;

4. di dare atto che le disposizioni operative sono assoggettate a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza almeno annuale.

5. di disporre che al presente provvedimento venga assicurata: a) la pubblicità legale con pubblicazione all’Albo Pretorio, nonché b) la massima diffusione presso tutto il personale operante presso l’Ente e presso tutti i soggetti esterni qualificabili in termini di responsabili del trattamento.

E con successiva votazione, favorevole ed unanime espressa in forma palese,

DELIBERA

Di dichiarare immediatamente eseguibile la presente deliberazione, ai sensi dell’art. 134, comma 4 del D. Lgs. 18.8.2000 n. 267.

Il presente verbale viene letto e sottoscritto come segue.

Il Sindaco	Il Segretario Comunale
F.to SEMINO FABIO	F.to Dott. GIOVANNI OLIVOTTO

REFERTO DI PUBBLICAZIONE (art.124, D.Lgs. 18.08.2000 n.267)

n. Registro delle Pubblicazioni

Certifico io sottoscritto Segretario Comunale su conforme dichiarazione del Messo, che copia del presente verbale è stato pubblicato il giorno 22.05.2024 all'Albo Pretorio ove rimarrà esposto per 15 giorni consecutivi.

Il Messo Comunale	Il Segretario Comunale
F.to GUGLIELMONE PIETRO	F.to Dott. GIOVANNI OLIVOTTO

CERTIFICATO DI ESECUTIVITA' (art. 134, D.Lgs. 18.08.2000, n. 267)

Si certifica che la suestesa deliberazione è divenuta esecutiva in data 20.05.2024

☒ Perchè dichiarata immediatamente eseguibile

☐ Perchè decorso il termine di 10 giorni dalla data di pubblicazione all'Albo Pretorio senza opposizioni

Il Segretario Comunale
F.to Dott. GIOVANNI OLIVOTTO

Copia conforme all'originale, in carta libera per uso amministrativo
Addi', 20.05.2024

IL SEGRETARIO COMUNALE
Dott. GIOVANNI OLIVOTTO