Comune di
VIGARANO MAINARDA

DELIBERA DI GIUNTA
N. 52 DEL 30/05/2019

Oggetto: APPROVAZIONE PROCEDURA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA (DATA BREACH)

L'anno 2019 addì 30 del mese di 05 alle ore 09:30 si è riunita la Giunta appositamente convocata.

All'appello risultano:

PARON BARBARA	Sindaco	Presente
TAGLIANI FLAVIO	Vice Sindaco	Assente
DE MICHELE AGNESE	Assessore	Presente
ZOBOLI ELENA	Assessore	Presente
BELLINI ANDREA	Assessore	Presente

Partecipa il Segretario Comunale MUSCO ANTONINO.

Accertata la validità dell'adunanza PARON BARBARA in qualità di Sindaco ne assume la presidenza, dichiarando aperta la seduta e invitando la Giunta a deliberare in merito all'oggetto sopra indicato.

La proposta in oggetto come di seguito riportata viene approvata con voti espressi in forma palese per il merito e successivamente e separatamente per l'immediata eseguibilità.

Unità Proponente: SETTORE AFFARI GENERALI - RISORSE UMANE - SERV. DEMOGRAFICI E CIMITERIALI - SERV. ALLA PERSONA

OGGETTO: APPROVAZIONE PROCEDURA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA (DATA BREACH)

LA GIUNTA COMUNALE

PREMESSO CHE:

il 24/05/2016 è entrato in vigore il Regolamento UE 2016/679 sulla protezione dei dati personali (di seguito, Regolamento UE o GDPR), che dispiega efficacia negli ordinamenti nazionali a partire dal 25/05/2018;

in data 19.9.18 è entrato in vigore il d.lgs. 10.8.18 n.101 di armonizzazione della normativa nazionale alle disposizioni del regolamento europeo 2016/679;

DATO ATTO CHE:

con Decreto del Sindaco di Vigarano Mainarda n.3 del 23.5.18, prot.7144 del 23.5.18, è stata designata Lepida spa quale Responsabile della protezione dei dati personali (RPD-DPO) del Comune di Vigarano Mainarda;

con deliberazione di giunta comunale n.68 del 26.6.18 è stato approvato il “modello organizzativo in materia di protezione dei dati personali" del Comune di Vigarano Mainarda ai sensi del regolamento UE 2016/679;

RICHIAMATI gli artt. 33 e 34 del regolamento UE 2016/679 che prevedono l’adozione da parte dei soggetti che trattano dati personali di specifiche procedure di gestione degli incidenti di sicurezza (c.d. data beach) in caso di violazione dei dati personali trattati;

RITENUTO di adottare la procedura per la gestione degli incidenti di sicurezza e per l’individuazione delle violazioni di dati personali oltre a definire le modalità di notifica all’Autorità Garante ed eventualmente anche agli interessati in caso si verifichi tale eventualità;

RITENUTO pertanto di approvare il documento inerente “PROCEDURA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA (DATA BREACH)” allegato al presente atto a costituirne parte integrante e sostanziale;

AD unanimità di voti,resi palesi

DELIBERA

1) per i motivi in premessa esposti, di approvare il documento inerente “PROCEDURA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA (DATA BREACH)” allegato al presente atto di cui costituisce parte integrante e sostanziale;

Comune di
VIGARANO MAINARDA

2) di trasmettere copia del presente atto al Responsabile della protezione dei dati personali (RPD-DPO) del Comune di Vigarano Mainarda;

3) di dare atto che sulla proposta della presente deliberazione è stato espresso il parere tecnico di cui all'art. 49 del D.lgs. 267/2000,che si allega al presente atto,di cui costituisce parte integrante e sostanziale;

4) con separata votazione palese,ad esito unanime,la presente deliberazione viene dichiarata immediatamente eseguibile,ai sensi dell'art. 134 comma 4 del D.lgs. 267/2000, stante l'urgenza di provvedere.

Approvato e sottoscritto con firma digitale:

Il Sindaco	Il Segretario Comunale
D.ssa PARON BARBARA	Dr. MUSCO ANTONINO

COMUNE DI VIGARANO MAINARDA

PROVINCIA DI FERRARA

PROCEDURA PER LA GESTIONE

DEGLI INCIDENTI DI SICUREZZA

(DATA BREACH)

INDICE

1. SCOPO

Il presente documento contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016.
Tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente devono essere informati e osservare la presente Procedura.

2. AGGIORNAMENTO

Il Referente dell'ente designato dal Titolare per la gestione degli incidenti di sicurezza (Referente data beach), nel caso di variazioni organizzative e/o normative, aggiorna la presente procedura e la propone in approvazione all'Organo competente affinché la renda esecutiva.

3. DEFINIZIONI

Le seguenti definizioni dei termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento europeo n. 679 del 2016:
«**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione,l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione,l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
«violazione dei dati personali»: 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 in formato elettronico e/o cartaceo;
«**Responsabile della Protezione dei Dati**»: incaricato di assicurare la corretta gestione dei dati personali nell'Ente;
«Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE.

4. ORGANIZZAZIONE DELLE ATTIVITÀ DI GESTIONE DELL'EVENTO VIOLAZIONE DEI DATI PERSONALI

Il Titolare deve:

- designare un Referente della gestione delle violazioni dei dati personali (di seguito Referente data breach);
- comunicare i nomi del designato a tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente;
- avvalendosi del Referente data breach, predisporre il Registro delle violazioni dei dati personali.

5. GESTIONE DELLE ATTIVITÀ CONSEGUENTI AD UNA POSSIBILE VIOLAZIONE DI DATI PERSONALI

Il soggetto che, a diverso titolo o in quanto autorizzato al trattamento di dati personali di cui è titolare l'Ente,viene a conoscenza di una possibile violazione dei dati personali, deve immediatamente segnalare l'evento al Referente data breach e fornirgli la massima collaborazione.
La mancata segnalazione del suddetto evento comporta a diverso titolo responsabilità a carico del soggetto che ne è a conoscenza.
Il Referente data breach, se del caso avvalendosi del Gruppo di gestione delle violazioni dei dati personali, composto da tutti i Responsabili di settore dell'ente,,deve:

- adottare le Misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, informare immediatamente il Responsabile della Protezione dei Dati per una valutazione condivisa;
- condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici,legali, ecc.) attraverso la compilazione del "Modello di potenziale violazione di dati personali al Responsabile Protezione Dati";
- riferire i risultati dell'indagine inviando il modello agli indirizzi segreteria@lepida.it e dpo-team@lepida.it al Responsabile della Protezione dei Dati e per conoscenza al Titolare.

Il Responsabile della Protezione dei Dati, ricevuti i risultati dell'indagine, analizza l'accaduto e formula un parere in merito all'evento, esprimendo la propria valutazione, non vincolante, che lo stesso configuri in una violazione dei dati personali e che possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche.
Lo invia quindi al Referente data breach che lo mette a conoscenza del Titolare.

6. NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ GARANTE

Il Titolare, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, e dalle valutazioni fatte dal Referente della gestione delle violazioni dei dati personali, se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione avvalendosi del "Modello comunicazione violazione all'Autorità Garante".
La notifica deve essere effettuata senza ingiustificato ritardo dall'accertamento dell'evento e, ove possibile,entro 72 ore dall'accertamento dello stesso con le modalità e i contenuti previsti dall'art. 33 del Regolamento europeo n. 679 del 2016.

7. COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI AGLI INTERESSATI

Il Titolare, accertata la violazione dei dati personali e ritenendo che la stessa possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, oltre alla notifica di cui al punto 6, decide le modalità di comunicazione di tale violazione agli interessati, come previsto dall'art. 34 del Regolamento europeo n. 679 del 2016.

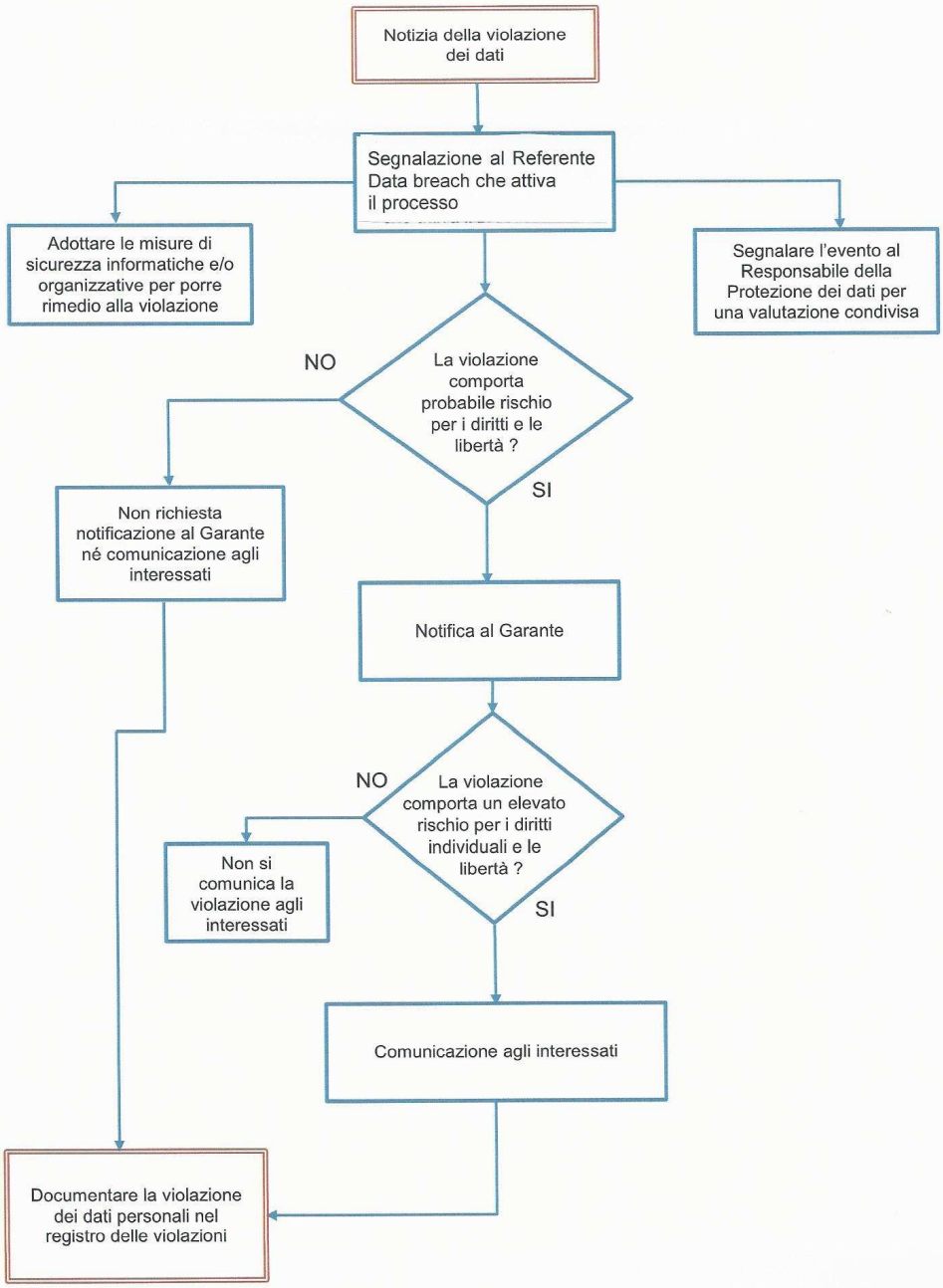
8. COMPILAZIONE DEL REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI

Il Titolare, avvalendosi del Referente data breach, documenta qualsiasi violazione dei dati personali,comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nel Registro delle violazioni dei dati personali.
Tale documento è tenuto e implementato dal Referente data breach e consente all'autorità di controllo di verificare il rispetto dall'art. 33 del Regolamento europeo n. 679 del 2016.
Per la redazione del registro è possibile ricorrere al sistema di fascicolazione se disponibile nel programma di gestione documentale dell'Ente o ad un file excel.
Allegati alla presente procedura:

- flusso degli adempimenti in caso di violazione dei dati (Allegato n.1);
- modello di potenziale violazione di dati personali al Responsabile Protezione Dati (Allegato n.2);;
- modello comunicazione violazione all'Autorità Garante (Allegato n.3);.

Allegato n.1

Il flusso degli adempimenti in caso di violazione dei dati



ALLEGATO N.2

POTENZIALE VIOLAZIONE DI DATI PERSONALI
MODELLO DI COMUNICAZIONE AL RESPONSABILE DELLA PROTEZIONE DEI DATI

Ente COMUNE DI VIGARANO MAINARDA

Referente data beach _____

Telefono _____ **Email** _____

Breve descrizione della violazione dei dati personali

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca di dati?

☐ Il _____
☐ Tra il _____ e il _____
☐ In un tempo non ancora determinato
☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio: tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)
☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
☐ Furto (i dati non sono più sui sistemi del titolare e non li ha l'autore della violazione)
☐ Altro _____

Dispositivo o strumento oggetto della violazione

☐ Computer
☐ Rete
☐ Dispositivo mobile
☐ File o parte di un file
☐ Strumento di backup
☐ Documento cartaceo
☐ Software _____
☐ Servizio informatico _____
☐ Altro _____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

☐ Numero _____ di persone
☐ Circa _____ persone
☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

☐ Dati anagrafici/codice fiscale
☐ Dati di accesso e di identificazione (*username, password, customer ID, altro*)
☐ Dati relativi a minori
☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale
☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
☐ Dati giudiziari

☐ Copia per immagine su supporto informatico di documenti analogici
☐ Ancora sconosciuto
☐ Altro _____

Fornitori o soggetti esterni coinvolti

Misure tecniche, informatiche e organizzative applicate ai dati oggetto di violazione

Vigarano Mainarda, _____

Firma _____

ALLEGATO N. 3

VIOLAZIONE DI DATI PERSONALI
MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dall'articolo art. 33 del GDPR, il Titolare è tenuto a comunicare all'Autorità Garante per la protezione dei dati personali agli indirizzi databreach.pa@pec.gpdp.it e protocollo@pec.gpdp.it le violazioni dei dati personali (*data breach*) di cui è titolare.

La comunicazione deve essere effettuata entro 72 ore dalla conoscenza del fatto.

ENTE TITOLARE DEL TRATTAMENTO

Denominazione o ragione sociale _____

Provincia_____ Comune _____

Cap _____ Indirizzo _____

Nome e Cognome della persona fisica addetta alla comunicazione _____
Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali contatti (altre informazioni) _____

Nome e dati contatto RPD _____

DENOMINAZIONE DELLA/E BANCA/BANCHE DATI OGGETTO DI DATA BREACH E BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI IVI TRATTATI

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca di dati?

☐ Il _____
☐ Tra il _____ e il _____
☐ In un tempo non ancora determinato
☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio: tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)
☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
☐ Furto (i dati non sono più sui sistemi del titolare e non li ha l'autore della violazione)
☐ Altro _____

Dispositivo o strumento oggetto della violazione

☐ Computer
☐ Rete
☐ Dispositivo mobile
☐ File o parte di un file
☐ Strumento di backup
☐ Documento cartaceo
☐ Software _____
☐ Servizio informatico _____
☐ Altro _____

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

☐ Numero _____ di persone
☐ Circa _____ persone
☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

☐ Dati anagrafici/codice fiscale
☐ Dati di accesso e di identificazione (*username, password, customer ID, altro*)
☐ Dati relativi a minori
☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale
☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
☐ Dati giudiziari
☐ Copia per immagine su supporto informatico di documenti analogici
☐ Ancora sconosciuto
☐ Altro _____

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

☐ Basso/trascurabile
☐ Medio
☐ Alto
☐ Molto alto

Misure tecniche, informatiche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il _____
☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Vigarano Mainarda, _____

Firma _____