COMUNE DI ROMAGNESE
PROVINCIA DI PAVIA

DELIBERAZIONE DELLA GIUNTA COMUNALE

NR. 60
DATA: 12/11/2025

OGGETTO: **APPROVAZIONE PROCEDURA PER LA GESTIONE DI DATA BREACH AI SENSI DEL REGOLAMENTO (UE) N.679/2016 (GDPR).**

LA GIUNTA COMUNALE

L'anno duemila**VENTICINQUE** il giorno **DODICI** del mese di **NOVEMBRE** alle ore **16:45** nella sala delle adunanze si è riunita la **GIUNTA COMUNALE,** regolarmente convocata nei termini di legge; Richiamato il Regolamento per il funzionamento della Giunta Comunale approvato con deliberazione della Giunta Comunale n. 32 del 30/03/2022;
Riunita in videoconferenza tramite l'applicativo Microsoft Teams;

Risultano presenti:

		PRESENTE	ASSENTE
1	**ACHILLE MANUEL – SINDACO** COLLEGATO TELEMATICAMENTE	X	
2	**GALLINI BENITO -VICE SINDACO**	X	
3	**MATTI ELISABETTA – ASSESSORE**	X	

Totale: Presenti n . 3 Assenti n. 0

PARTECIPA ALLA SEDUTA, il Segretario Comunale Dott. Sebastiano Tomagra.
Il Presidente Sig. Achille Manuel nella sua qualità di Sindaco, COLLEGATO TELEMATICAMENTE, dopo aver constatato la validità dell'adunanza dichiara aperta la seduta ed invita gli intervenuti a discutere ed a deliberare sulla proposta di cui all'argomento in oggetto.

LA GIUNTA COMUNALE

Visto il Regolamento per il funzionamento della Giunta Comunale approvato con deliberazione della Giunta Comunale n. 32 del 30.03.2022;

Dato atto che la Giunta Comunale è riunita in videoconferenza tramite l'applicativo Microsoft Teams;

RILEVATO che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale é 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;

CONSIDERATO che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:

- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

TENUTO PRESENTE che tale evoluzione ha indotto l'Unione europea ad adottare 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 (di seguito solo "GDPR");

DATO ATTO che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

RILEVATO che con il GDPR è stato richiesto agli Stati membri:

- un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

VISTO il D.lgs 196/2003, modificato dal D.Lgs. 10 agosto 2018 n. 101;

DATO ATTO che il GDPR introduce l'obbligo di notificare all'autorità di controllo nazionale (Garante Privacy) incidenti sulla sicurezza che comportino la violazione dei dati personali (data breach) e di rendere nota la violazione stessa alle persone fisiche interessate;

DATO ATTO che la notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- descrizione della natura della violazione dei dati personali e le registrazioni dei dati personali in questione;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o da adottare da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

TENUTO PRESENTE che la violazione dei dati personali è da intendersi come 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 tale da impedire al titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR;

DATO ATTO che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo, e che tale comunicazione deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali, contenendo obbligatoriamente i seguenti contenuti minimi:

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

RILEVATO che, per quanto sopra, è necessario istituire:

1. una Procedura data breach
2. un registro interno data breach, dove vengono annotate sia le violazioni non notificabili che quelle notificabili, il quale deve contenere i seguenti dati:
   - i dettagli relativi alla violazione (cause, fatti e dati personali interessati);
   - gli effetti e le conseguenze della violazione;
   - i provvedimenti adottati per porvi rimedio;
   - il ragionamento alla base delle decisioni prese in risposta a una violazione (con particolare riferimento alle violazioni non notificate ed alle violazioni notificate con ritardo);

DATO ATTO che la Procedura data breach, avente lo scopo di indicare le modalità di gestione del *data breach, garantisce* la realizzabilità tecnica e la sostenibilità organizzativa;

DATO ATTO che è stato individuato quale responsabile del procedimento, la figura del Segretario Comunale e che lo stesso, al fine di garantire la massima diffusione interna ed esterna e la massima conoscibilità sulle azioni da intraprendere e sui comportamenti da adottare in caso di data breach, è tenuto a garantire la pubblicazione della Procedura data breach sul sito web istituzionale nella sezione "Amministrazione Trasparente", sottosezione di primo livello "Altri Contenuti", sottosezione di secondo livello "Privacy", nonché a garantire la conoscibilità della stessa a tutti i dipendenti dell'Ente;

VISTI:
- D.Lgs. 267/2000 e s.m.i.;
- D.Lgs. 196/2003 e s.m.i.;
- D.Lgs 101/2018 e s.m.i.
- D.Lgs. 33/2013 e s.m.i.;
- Regolamento (UE) n. 679/2016;

Acquisiti il parere favorevole di regolarità tecnica amministrativa espresso dal Segretario Comunale ai sensi dell'art. 49 comma 1 del D.Lgs 267/2000;

Con voti unanimi espressi ai sensi di legge;

DELIBERA

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

1. **DI APPROVARE** la Procedura per la gestione di ***data breach*** ai sensi del Regolamento (UE) n.679/2016, allegata alla presente, per formarne parte integrante e sostanziale;
2. **DI DARE ATTO** che il Responsabile del Procedimento è individuato nella figura del Segretario Comunale;

Successivamente con separata ed unanime votazione favorevole, resa ai sensi di legge

DELIBERA

Di dichiarare la presente deliberazione immediatamente eseguibile ai sensi dell'art. 134, comma 4, del D.Lgs 267/2000.

ALLEGATO ALLA DELIBERA DELLA GIUNTA COMUNALE N. 60 DEL 12/11/2025

RESPONSABILI DEI SERVIZI

****

PARERE DI REGOLARITA' TECNICO - AMMINISTRATIVA

Visto l'art.49 comma 2 del T.U.E.L.approvato con D.Lgs.267 DEL 18.08.2000 ,il sottoscritto Segretario Comunale esprime parere favorevole,in ordine alla regolarità Tecnico amministrativa della proposta di deliberazione in oggetto.

Lì 12/11/2025

IL SEGRETARIO COMUNALE
DOTT. SEBASTIANO TOMAGRA

PROCEDURA DATA BREACH

Sommario

1. PREMESSA

Il Comune di Romagnese, ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuta 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 (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati). È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici al Comune di Romagnese e per poter comunicare nei tempi e nei modi previsti dalla normativa europea all'Autorità Garante e/o agli interessati. Le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo al Comune di Romagnese di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del "fatturato" annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

2. SCOPO

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni di dati personali trattati dall'Ente in qualità di Titolare del trattamento (di seguito "Titolare del trattamento"). Queste procedure sono ad integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della normativa vigente.

3. COS'E UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere a titolo esemplificativo e non esaustivo:

a. Divulgazione di dati personali a soggetti non autorizzati;
b. Perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
c. Perdita o furto di documenti cartacei;
d. Infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
e. Accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
f. Casi di pirateria informatica (usurpazione delle credenziali di accesso – fishing);
g. Banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
h. Virus o altri attacchi al sistema informatico o alla rete aziendale;
i. Violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate);
j. Smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
k. Invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

4. A CHI SONO RIVOLTE QUESTE PROCEDURE?

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) quali: a)

a. 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 delle prestazioni richieste per conto del Titolare del trattamento (di seguito denominati Destinatari interni);
b. qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno 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 (di seguito genericamente denominati Destinatari esterni);

Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi o mezzi che ne assicurino la comprensione.

Il rispetto della presente 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.

5. A QUALI TIPI DI DATI SI RIFERISCONO QUESTE PROCEDURE?

Queste procedure si riferiscono a:

a. Dati personali trattati "da" e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
b. Dati personali conservati o trattati a mezzo di qualsiasi altro Sistema in uso nel Comune di Romagnese.

Per «dato personale» si intende: 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.

6. GESTIONE COMUNICAZIONE DI DATA BREACH

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del DPO.

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il superiore gerarchico il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Titolare del trattamento o un suo delegato mediante la compilazione dell'Allegato A – Modulo di comunicazione interna di Data Breach da inviare a mezzo mail all'indirizzo:

comune.romagnese@virgilio.it

7. GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti cinque step:

Step 1: Identificazione e indagine preliminare;

Step 2: Contenimento, recovery e risk assessment;

Step 3: Eventuale notifica all'Autorità Garante;

Step 4: Eventuale comunicazione agli interessati;

Step 5: Documentazione della violazione.

Step 1: Identificazione e indagine preliminare

L'Allegato A, debitamente compilato, permetterà al Titolare del trattamento o un suo delegato, di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2) e con il coinvolgimento del DPO. Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o un suo delegato dovrà coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile dell'Area IT o un suo delegato in caso di assenza. Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato A, quali:

- la data di scoperta della violazione (tempestività);
- Il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento o un suo delegato insieme al DPO dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso... ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il DPO valuteranno la gravità della violazione utilizzando l'Allegato B - Modulo di valutazione del Rischio connesso al Data Breach, che dovrà essere esaminato unitamente all'Allegato A, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 GDPR . Se, infatti, gli obblighi di notifica all'Autorità di Controllo

scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Step 3: Eventuale notifica all'Autorità Garante competente

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, il Comune di Romagnese provvederà, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

Pertanto, il Titolare del trattamento e il DPO individueranno l'Autorità di Controllo competente sulla base delle informative e/o della valutazione d'impatto sulla protezione dei dati già in essere presso l'ente in relazione ai dati oggetto di violazione.

Una volta determinata l'Autorità di Controllo competente, il Titolare del Trattamento e il DPO individuano la corretta modulistica da utilizzare per effettuare la notificazione e vi provvederanno.

Per la notifica all'Autorità Garante Italiana si potrà utilizzare il "*Modello notifica Data Breach*" fornito dal Garante all'indirizzo:

https://servizi.gpdp.it/databreach/s/

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, il Comune di Romagnese dovrà provvedervi, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare del trattamento o da un suo delegato e il DPO dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o da un suo delegato e il DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e- mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso l'Allegato A, il Comune di Romagnese sarà tenuto a documentarlo. Tale documentazione sarà affidata al Titolare del trattamento o da un suo delegato con l'ausilio del Fornitore Sistemi Informatici (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta del Registro dei Data Breach, secondo le informazioni ivi riportate: (i) n. violazione; (ii) data violazione; (iii) natura della violazione; (iv) categoria di interessati; (v) categoria di dati personali coinvolti; (vi) numero approssimativo di registrazioni dei dati personali; (vii) conseguenze della violazione; (viii) contromisure adottate; (ix) se sia stata effettuata notifica all'Autorità Garante Privacy; (x) se sia stata effettuata comunicazione agli interessati. Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante, qualora l'Autorità chieda di accedervi.

ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH

Qualora scopra un Data Breach, è pregato di informare immediatamente il Suo superiore gerarchico, il quale, a sua volta, dovrà compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo email:

comune.romagnese@virgilio.it

Comunicazione di Data Breach	**Note**
Data scoperta violazione: **Data dell'incidente:** **Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):**	
Nome della persona che ha riferito della violazione:	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): ***In caso di destinatario esterno indicare la ragione sociale*:**	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	

Responsabile della struttura:
Data:

ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

Assessment di gravità	**A cura del DPO insieme con ASICT (se del caso) e il Responsabile dell'ufficio coinvolto della violazione**
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): lettura (presumibilmente i dati non sono stati copiati), copia (i dati sono ancora presenti sui sistemi ma del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	

Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?

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

La violazione può avere conseguenze negative in uno dei seguenti settori aziendali: operation, research, financial, legal, liability or reputation?

Qual è la natura dei dati coinvolti? Compilare le sezioni sottostanti:

- **Dati personali generici:**

- **I dati particolari (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile:**

a) **origine razziale o etnica;**
b) **opinion politiche, convinzioni religiose o filosofiche;**
c) **appartenenza sindacale;**
d) **dati genetici;**
e) **dati biometrici;**
f) **dati giudiziari;**
g) **relative alla salute o all'orientamento sessuale di una persona.**

- **Informazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito);**

- **Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori);**

- **Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone;**

- **Altro:**

La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?

Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?

Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (i.e. La pseudonimizzazione e la cifratura dei dati personali)

Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?

Classificazione della violazione (1, 2 o 3) e Motivazioni:

Notificazione del Data Breach all'Autorità Garante Si/NO **Si/NO Se sì, notificato in data: Dettagli:**

Comunicazione del Data Breach agli interessati	**Si/NO Se sì, notificato in data: Dettagli:**
Comunicazione del Data Breach ad altri soggetti	**Si/NO Se sì, notificato in data: Dettagli:**

COPIA

Letto, approvato e sottoscritto.

IL SINDACO
DOTT. MANUEL ACHILLE

IL SEGRETARIO COMUNALE
DOTT. SEBASTIANO TOMAGRA

****

DICHIARAZIONE DI PUBBLICAZIONE

Si dichiara che copia della presente deliberazione è stata **pubblicata all'albo pretorio** per giorni **15** consecutivi dal_____

Addì_____

IL SEGRETARIO COMUNALE
DOTT. SEBASTIANO TOMAGRA

****

Per copia conforme all'originale.

Lì 19 NOV. 2025

IL SEGRETARIO COMUNALE
DOTT. SEBASTIANO TOMAGRA

La presente è stata comunicata, ai sensi dell'art.125 del D.Lgs. n.267/2000 ai Capigruppo Consiliari in data: 19 NOV. 2025

****

DICHIARAZIONE DI ESEGUIBILITA'

La presente è stata dichiarata immediatamente eseguibile ai sensi del 4° comma dell'art.134 D.Lgs. n.267/2000.

Lì_____

IL SEGRETARIO COMUNALE
DOTT. SEBASTIANO TOMAGRA

DICHIARAZIONE DI ESECUTIVITA'

La presente divenuta esecutiva il_____ai sensi del 3° comma dell'art.134 D.Lgs. n.267/2000.

Lì_____

IL SEGRETARIO COMUNALE
DOTT. SEBASTIANO TOMAGRA