COMUNE DI SAN MARTINO DI LUPARI
(Provincia di Padova)

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DEI DATI

Revisione:	--
Data di revisione:	--
Redatta da:	Segretario Generale
Approvata da:	Giunta Comunale con delibera n. 184 del 19.12.2019

PREMESSA

La presente procedura viene applicata in ottemperanza al rispetto delle misure minime di sicurezza adottate dal Comune di San Martino di Lupari.

I dati informatici devono essere contenuti in un sistema Data Base /Gestionale possibilmente criptato, con profilazione utenti e credenziali di accesso univoche per ogni utente.

1. CAMPO DI APPLICAZIONE E DESTINATARI

Scopo della presente procedura è di descrivere le attività da svolgersi in caso di violazione di dati personali (c.d. Data Breach).

Si intende per violazione di dati qualsiasi 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 dall'Amministrazione comunale.

Rientra pertanto nella nozione di violazione di dati qualsiasi incidente o qualsiasi evento che possa determinare la compromissione:

a) della integrità e dell'esattezza dei dati personali, ovvero che possa distruggere o alterare i dati personali trattati (es. distruzione di archivi o documenti cartacei, modifiche accidentali ai dati registrati, rottura di dispositivi di archivazione);
b) della disponibilità dei dati personali, ovvero che possa determinare l'impossibilità di accedere ai dati personali per un periodo di tempo apprezzabile qualora dall'indisponibilità dei dati derivi l'impossibilità di effettuare i trattamenti per i quali i dati sono trattati (es. malfunzionamento dei sistemi informatici che impedisca di svolgere l'attività degli uffici);
c) della riservatezza dei dati trattati, ovvero che determini l'accesso ai dati da parte di soggetti non autorizzati (es. accesso abusivo ai sistemi informatici o comunicazione involontaria dei dati personali per notifica di un provvedimento al destinatario errato).

La Procedura definisce i principi e le azioni generali per gestire la violazione dei dati personali e adempiere agli obblighi relativi alla notifica alle Autorità di Controllo e ai singoli individui, come richiesto dal Regolamento (UE) 2016/679.

Tutto il personale a tempo indeterminato e determinato, i collaboratori e terzi che lavorino o agiscano per conto del Comune di San Martino di Lupari, deve obbligatoriamente essere a conoscenza e seguire la presente procedura in caso di violazione dei dati personali.

A tal fine il Comune di San Martino di Lupari rende idonea pubblicità mediante pubblicazione del presente documento sul sito istituzionale e diffusione via email dello stesso ai propri dipendenti\consulenti\collaboratori o terzi che agiscano\lavorino per l'Ente non appena prendano servizio.

2. DOCUMENTI DI RIFERIMENTO

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo 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);
- Politica sulla Protezione dei Dati Personali;

- Guidelines on Personal data breach notification under Regulation 2016/679 - *ARTICLE 29 DATA PROTECTION WORKING PARTY;*
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015 (Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015).

3. DEFINIZIONI

Le seguenti definizioni ed i termini utilizzati in questo documento, sono tratte dall'articolo 4 del Regolamento (UE) 2016/679 ovvero afferiscono ad elementi disciplinati nel presente documento:

- **«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 ed applicate ai 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;
- **«titolare del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri. Per il Comune di San Martino di Lupari **«titolare del trattamento»** è il Comune di San Martino di Lupari in persona del proprio legale rappresentante pro tempore: il Sindaco. Le funzioni in materia di organizzazione dei trattamenti di dati personali proprie del titolare sono svolte dalla Giunta comunale.
- **«responsabile del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Per il Comune di San Martino di Lupari **«responsabile del trattamento»** è la qualificazione di tutti i soggetti che trattano dati personali per conto del titolare del trattamento quali: altre autorità pubbliche, la società partecipata in house providing, le software house utilizzate, le società di elaborazione dei dati comunque denominate…
- **«DPO data protection officer»** (o responsabile della protezione dei dati - RDP) è un consulente tecnico designato dal Titolare del Trattamento, le cui competenze sono disciplinate dalla norma GDPR;
- **«Gruppo di Risposta alle Violazioni dei Dati»**: esplica la sua funzione consultiva in caso di c.d. Data Breach ed è costituito dal Sindaco, dal Segretario, dall'Amministratore di Sistema, dal responsabile della Transizione Digitale del Comune di San Martino di Lupari, e dal DPO.
- **«autorità di controllo»:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 (Garante dei dati personali)

4. GRUPPO DI RISPOSTA ALLE VIOLAZIONI DEI DATI

Il Sindaco del Comune di San Martino di Lupari in qualità di Titolare del trattamento provvede, con proprio atto, alla nomina dei componenti del Gruppo di Risposta alle Violazioni dei Dati, come individuati nel precedente punto 3. Il Gruppo deve essere nominato a prescindere dal fatto che una violazione sia avvenuta o meno.

Il Segretario Comunale dirige e presiede le attività del Gruppo. In caso di assenza o impedimento ne farà le veci il di lui sostituto.

Le riunioni del gruppo possono svolgersi anche in audio\video conferenza e sono valevoli anche in assenza di alcuni componenti.

Il gruppo deve essere convocato a fronte di ogni segnalazione relativa ad una sospetta violazione di dati personali.

La missione del gruppo è di fornire una risposta immediata, efficace ed esperta a qualsiasi sospetta, presunta o effettiva violazione dei dati personali che riguardi l'Amministrazione.

Il Gruppo di Risposta alle Violazioni dei Dati può trattare più di una violazione dei dati personali sospetta, presunta o effettiva alla volta.

Il Gruppo di Risposta alle Violazioni dei Dati presta ai sensi di legge la propria attività consulenziale in ordine a violazioni di dati personali presunte, sospette o effettive. A tal fine ciascun componente rende disponibili i propri dati, compresi quelli personali di recapito, al Segretario Comunale, nonché gli altri membri del gruppo. Le informazioni di contatto acquisite verranno pertanto a tal fine archiviate ed utilizzate unicamente per lo scopo previsto.

5. COMPITI DEL GRUPPO

Il Gruppo di Risposta alle Violazioni dei Dati coadiuva il Titolare del trattamento nella risoluzione delle questioni relative ad un evento di cd data breach sospetto, presunto o effettivo, esprimendosi in relazione ai seguenti punti (elenco esemplificativo non esaustivo) ove applicabili:

1. Determinare se la violazione di cui trattasi debba o meno essere considerata una violazione dei dati personali;
2. Valutare se la violazione debba essere notificata all'Autorità di controllo o comunicata agli interessati
3. Convalidare / assegnare un livello di urgenza alla violazione dei dati personali;
4. Assicurare che sia avviata, condotta, documentata e conclusa un'indagine corretta e imparziale (compresa l'informatica forense, se necessario);
5. Identificare i requisiti per la risoluzione e monitorare la soluzione;
6. Coordinarsi con le autorità competenti;

6. PROCESSO DI RISPOSTA ALLE VIOLAZIONI DEI DATI

Il Processo di Risposta alle Violazioni dei Dati è articolato come segue:

1. Il dipendente dell'Amministrazione che si accorge di una violazione o perdita dei dati (informatici o cartacei) informa immediatamente via email il suo Responsabile di Area relazionando quanto segue:
   a. Breve descrizione dei fatti che danno luogo alla sospetta violazione;
   b. Indicazione del/dei documento/documenti e/o della/e banca/banche dati oggetto di data breach;
   c. Indicazione, anche approssimativa o presuntiva, del tempo in cui si è verificata la violazione dei dati personali;
   d. Luogo dove è avvenuta la violazione dei dati (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili).

2. Il Responsabile di Area informa dell'evento il Segretario Comunale. Questi, assunte eventuali ulteriori informazioni qualora ritenute necessarie, convoca il Gruppo di Risposta alle Violazioni dei Dati, di cui il rappresentante legale pro tempore dell'Ente Titolare del trattamento fa parte.

3. Il Gruppo di Risposta alle Violazioni dei Dati procede tempestivamente alla seguente valutazione:
   a. Natura della violazione
      - Perdita di confidenzialità
      - Perdita di integrità
      - Perdita di disponibilità
   b. Causa della violazione
      - Azione intenzionale interna
      - Azione accidentale interna
      - Azione intenzionale esterna
      - Azione accidentale esterna
      - Sconosciuta
      - Altro (specificare)
   c. Categorie di dati personali coinvolti nella violazione
      - Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice
      - fiscale, altro...)
      - Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso
      - o mobile)
      - Dati di accesso e di identificazione (username, password, customer ID, altro…)
      - Dati di pagamento (numero di conto corrente, dettagli della carta di credito,
      - altro…)
      - Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di
      - traffico, dati relativi alla navigazione internet, altro…)
      - Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
      - Dati di profilazione
      - Dati relativi a documenti di identificazione/riconoscimento (carta di identità,
      - passaporto, patente, CNS, altro…)
      - Dati di localizzazione
      - Dati che rivelino l'origine razziale o etnica
      - Dati che rivelino opinioni politiche
      - Dati che rivelino convinzioni religiose o filosofiche
      - Dati che rivelino l'appartenenza sindacale
      - Dati relativi alla vita sessuale o all'orientamento sessuale
      - Dati relativi alla salute
      - Dati genetici
      - Dati biometrici
      - Altro
   d. 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 li ha l'autore della violazione)
- Altro

e. Dispositivo oggetto della violazione
- Computer
- Rete
- Dispositivo mobile
- File o parte di un file
- Strumento di *backup*
- Documento cartaceo
- Altro da specificare

f. Categorie di interessati coinvolti
- Dipendenti/Consulenti
- Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
- Associati,soci, aderenti, simpatizzanti, sostenitori
- Soggetti che ricoprono cariche sociali
- Beneficiari o assistiti
- Minori
- Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- Altro

g. Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati;
h. Possibili conseguenze della violazione dei dati personali sui diritti e sulle libertà degli interessati e indicazione di un livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati;
i. Analisi delle misure tecniche e organizzative applicate ai dati oggetto di violazione.

4. Al termine della valutazione effettuata dal Gruppo di Risposta alle Violazioni dei Dati, il Titolare del Trattamento decide quanto segue:
   a. Se procedere alla notifica della violazione all'Autorità di controllo;
   b. Se comunicare o meno agli interessati l'evento di data breach
   c. Le misure tecnologiche e organizzative assunte o da assumere per contenere la violazione dei dati e prevenire simili violazioni future.

5. Il Gruppo di Risposta alle Violazioni dei Dati, entro 70 ore da quando è stata ricevuta la segnalazione di una possibile violazione deve fornire al Titolare un parere se:
   a. è necessario procedere alla notificazione della violazione all'Autorità di Controllo;
   b. è necessario procedere alla comunicazione della violazione agli interessati.

6. Il Gruppo di Risposta alle Violazioni di Dati provvede inoltre a suggerire eventuali misure urgenti da porre in essere per limitare l'impatto della violazione sui diritti e le libertà degli interessati.

7. NOTIFICA DI VIOLAZIONE DI DATI PERSONALI EFFETTUATA DAL RESPONSABILE DEL TRATTAMENTO

Qualora la violazione dei dati personali o la sospetta violazione dei dati riguardi i dati personali elaborati per conto di terzi, il Responsabile del trattamento informa il rispettivo titolare del

trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza dell'evento di data breach.

La notifica di cui sopra deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) 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 anche, se del caso, per attenuarne i possibili effetti negativi.

Il titolare del trattamento, coadiuvato dal Segretario Comunale e dal DPO, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di porre in essere le proprie attività di verifica in ordine al rispetto dei dettami di cui al GDPR.

8. NOTIFICA DI UNA VIOLAZIONE DI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO (GARANTE PER LA PROTEZIONE DEI DATI)

In caso di violazione dei dati personali, il titolare del trattamento notifica all' Autorità di Controllo (Garante per la protezione dei dati) la violazione dei dati personali (data breach) 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.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Nei casi più gravi, 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 è obbligato a comunicare la violazione anche alla persona a cui si riferiscono i dati (c.d. Interessato), senza ingiustificato ritardo, così come meglio disciplinato al successivo art.9.

In caso di violazione o sospetta violazione dei dati personali trattati dall'Amministrazione, il Titolare del Trattamento, coadiuvato dal Gruppo di Risposta alle Violazioni dei Dati avente funzione tecnico - consultiva, provvederà ad assumere le seguenti decisioni:

a) stabilire se la violazione dei dati personali debba essere segnalata all'Autorità di Controllo "Garante per la protezione dei dati" ed in caso affermativo provvedere alla relativa notifica senza indebito ritardo, e non oltre le 72 ore, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio per i diritti e le libertà degli interessati colpiti dalla violazione dei dati personali;

b) stabilire, a seguito della Valutazione d'Impatto sulla Protezione dei Dati avente ad oggetto

l’attività di trattamento interessata dalla violazione dei dati, se sia o meno necessario provvedere alla notifica della violazione agli interessati.

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) 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 anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite all’Autorità Garante in fasi successive senza ulteriore ingiustificato ritardo.

Il titolare del trattamento, coadiuvato dal Segretario Comunale e dal DPO, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di porre in essere le proprie attività di verifica in ordine al rispetto dei dettami di cui al GDPR.

9. COMUNICAZIONE DI VIOLAZIONE DI DATI PERSONALI ALL’INTERESSATO

Il Titolare del Trattamento dei dati personali, in collaborazione con il Gruppo di Risposta alle Violazioni dei Dati Personali, deve valutare se la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà dell'interessato. In caso affermativo, il Titolare del Trattamento deve informare gli interessati senza indebito ritardo.

La comunicazione agli interessati deve essere scritta in un linguaggio chiaro e semplice e deve contenere:

a) il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;

b) la descrizione delle probabili conseguenze della violazione dei dati personali;

c) la descrizione delle misure adottate o di cui il titolare del trattamento propone l'adozione per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Se il numero di interessati è sproporzionatamente elevato per poter informare singolarmente tutti i soggetti in questione, il Titolare dei dati personali adotta le misure necessarie per garantire che le persone interessate siano informate utilizzando canali appropriati e pubblicamente disponibili.

Non è richiesta la comunicazione all'interessato se viene soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

10. REGISTRO DELLE VIOLAZIONI

Ogni violazione dei dati personali che sia stata valutata come effettiva dal Gruppo di Risposta alle Violazioni dei Dati, anche se non notificata all'Autorità di Controllo o comunicata agli interessati dovrà essere registrata a cura del Titolare nel Registro delle violazioni istituito presso l'Amministrazione.

Le violazioni registrate sono prese in considerazione anche al fine dell'aggiornamento delle misure organizzative e tecniche.

12. MONITORAGGIO

Il Titolare del Trattamento, con l'ausilio del DPO e del Gruppo di Risposta alle Violazioni dei Dati, provvede al monitoraggio delle conseguenze delle violazioni dei dati personali scoperte ed all'eventuale aggiornamento delle misure di mitigazione e di prevenzione per un periodo di 12 mesi dalla scoperta della violazione.

Nel caso di violazioni di particolare gravità, il monitoraggio può essere prolungato.

13. RESPONSABILIZZAZIONE

Qualsiasi soggetto che commetta violazioni di legge in merito alla procedura descritta, sarà sottoposto alle misure disciplinari interne, sino alla risoluzione del rapporto di lavoro. Qualora si ravvisi che le sue azioni, siano in violazione di legge, potrà incorrere nelle responsabilità civili o penali previste.

14. GESTIONE DELLE REGISTRAZIONI SULLA BASE DEL PRESENTE DOCUMENTO

Nome del documento	Tempo di archiviazione
Elenchi delle persone da chiamare e sostituzioni	Permanente
Informazioni di contatto	Permanente
Decisioni documentate del Gruppo di Risposta alle Violazioni dei dati	5 anni
Comunicazione di una Violazione dei Dati	5 anni
Registro delle Violazioni di Dati	Permanente

12. VALIDITA' E GESTIONE DEL PRESENTE DOCUMENTO

Questo documento è stato approvato con deliberazione di Giunta Comunale n. 184 del 19.12.2019 ed è divenuto efficace a partire dal 19.12.2019.

Il responsabile per questo documento è il Titolare del trattamento, il quale deve controllare il documento con frequenza almeno annuale ed, ove necessario, provvedere alle eventuali modificazioni.

REGISTRO DELLE VIOLAZIONI															
Titolare del trattamento			Data Protection Officer / Privacy												
Nome			Nome												
Indirizzo			Indirizzo												
email			email												
Pec			telefono		Ultimo aggiornamento										
Numero	Descrizione della violazione	Data presunta della violazone	Data della scoperta	Luogo della violazione	Natura e tipologia dei dati anche solo presumibilmente coinvolti	Strumenti di elaborazione o di memorizzazione dei dati coinvolti	Categorie di interessati coinvolti	Numero approssimativo di interessati coinvolti	Numero approssimativo di registrazioni di dati coinvolti	probabili conseguenze della violazione dei dati personali	Misure di mitigazione coinvolte	Notifiazione al Garante?	Comunicazione agli interessati?	Motivi di esclusione della comunicazione/notificazione	