ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DEI DATI (Data Breach)

Redatto da R.DIENA

Approvato dal Comune di Pessinetto rappresentato dal Sindaco pro tempore Gianluca Togliatti il 30/11/2023

PREMESSA

La presente procedura viene applicata in ottemperanza al rispetto delle misure minime di sicurezza adottate dal Comune di Pessinetto

I dati informatici sono contenuti in server comunali, 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).

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 e s.m.i.

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

A tal fine il Comune rende idonea pubblicità mediante pubblicazione del presente documento anche con diffusione via e-mail dello stesso ai propri dipendenti/consulenti/collaboratori o terzi che agiscano/lavorino per la Società 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)

Guidelines on Personal data breach notification under Regulation 2016/679 - ARTICLE 29;

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 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.

- «titolare del trattamento» è il Comune di Pessinetto;
- «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;
- «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;
- «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 comunale, dal DPO, dall'Agente di Polizia locale , dall' esperto informatico, dall'amministratore di sistema e dal Consulente Privacy;
- «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 Gruppo di Risposta alle Violazioni dei Dati è costituito dai componenti prima dettagliati. Le riunioni del gruppo possono svolgersi anche in audio/video conferenza e sono valevoli anche in assenza di alcuni componenti.

Il gruppo può essere convocato ad esplicitare la propria funzione consultiva in ordine a qualsiasi sospetta o presunta violazione dei dati personali.

In tal senso il gruppo deve garantire la prontezza necessaria per una risposta alla violazione dei dati personali, insieme alle risorse e alla preparazione.

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

Se ritenuto opportuno e necessario possono essere coinvolti nelle attività del gruppo anche ulterior esperti interni o esterni allo scopo di gestire una specifica violazione dei dati personali (ad esempio, un fornitore di sicurezza informatica per svolgere attività di informatica forense o un'agenzia di comunicazione esterna per assistere in necessità di comunicazione di crisi).

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.

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. Convalidare / assegnare un livello di urgenza alla violazione dei dati personali; 3. Assicurare che sia avviata, condotta, documentata e conclusa un'indagine corretta e imparziale (compresa l'informatica forense, se necessario);
4. Identificare i requisiti per la risoluzione e monitorare la soluzione;
5. Coordinarsi con le autorità competenti;
6. Coordinare le comunicazioni interne ed esterne;
7. Assicurarsi che gli interessati siano adeguatamente informati.

Il Gruppo di Risposta alle Violazioni dei Dati viene attivato a seguito di un "ammissibilità preventiva" di un potenziale “data breach”, valutato in via informale dal consulente informatico

PROCESSO DI RISPOSTA ALLE VIOLAZIONI DEI DATI

Il Processo di Risposta alle Violazioni dei Dati viene avviato quando il dipendente viene a conoscenza che una sospetta, presunta o effettiva violazione dei dati personali si sia verificata. Di detto evento il dipendente deve dare immediata comunicazione al proprio Responsabile.

Il Responsabile provvederà a dare comunicazione del sospetto, presunto o effettivo “data breach” al consulente informatico che verificherà l’ammissibilità preventiva del presunto “data breach”. Qualora l’ammissibilità del presunto “data breach” sia positiva sarà informato il Gruppo di Risposta alle Violazioni dei Dati.

Il Segretario comunale, è incaricato della raccolta delle decisioni del gruppo, che costituiscono documentazione che potrebbe essere esaminata dalle autorità di controllo e, in quanto tale, da redigersi in modo preciso ed accurato per garantire la tracciabilità e la responsabilizzazione, ferma restando la competenza e responsabilità del Titolare del trattamento in ordine all’assunzione della decisione definitiva.

5. FASI DEL PROCESSO

1. Il dipendente che si accorge di una violazione o perdita dei dati (informatici o cartacei) informa immediatamente via email il suo Responsabile relazionando quanto segue:

   a. denominazione della/e banca/banche dati oggetto di *“data breach”*;

   b. breve descrizione della violazione dei dati personali ivi trattati;

   c. quando si è verificata la violazione dei dati personali trattati nell’ambito della banca dati;

   d. dove è avvenuta la violazione dei dati (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili).

2. Il Sindaco/Segretario comunale informa dell’evento il consulente informatico che congiuntamente al D.P.O., verificheranno l’ammissibilità preventiva del presunto “data breach”.

Qualora l’ammissibilità del presunto “data breach” sia positiva il Sindaco, assunte eventuali ulteriori informazioni qualora ritenute necessarie, convoca il Gruppo di Risposta alle Violazioni dei Dati.

3. Il Gruppo di Risposta alle Violazioni dei Dati procede tempestivamente alla seguente valutazione:

a. 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

b. Dispositivo oggetto della violazione
   - Computer
   - Rete
   - Dispositivo mobile
   - file o parte di un file
   - Strumento di backup
   - Documento cartaceo

- Altro da specificare

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

d. Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati;

e. 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 comunicare o meno agli interessati l'evento di "data breach"

b. le misure tecnologiche e organizzative assunte o da assumere per contenere la violazione dei dati e prevenire simili violazioni future.

5. Sulla base delle indicazioni raccolte, il Titolare del Trattamento procede alla compilazione della modulistica prevista dall'Autorità di Controllo (Garante per la protezione dei dati), e nel tempo stabilito, invia a mezzo pec al Garante le violazioni dei dati personali ("data breach")

6. 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 o dipendente informa il 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 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 pone rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

Il titolare del trattamento 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.

7. 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, coadiuvato dal D.P.O., 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 di seguito disciplinato all'art. 9 del presente documento.

In caso di violazione o sospetta violazione dei dati personali trattati, 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 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 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.

Nome del documento	**Tempo di archiviazione** ***(data retention)***
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

8. COMUNICAZIONE DI VIOLAZIONE DI DATI PERSONALI: IL TITOLARE DEL TRATTAMENTO DEI DATI 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 presso cui ottenere più informazioni;

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

c) la descrizione delle le 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

9. RESPONSABILIZZAZIONE

Qualsiasi soggetto che commetta violazioni di legge in merito alla procedura descritta, sarà sottoposto alle misure disciplinari interne, in riferimento a quanto previsto dal Codice di comportamento di cui alla Delibera della Giunta comunale n. 9 del 23/03/2023. Qualora si ravvisi che le sue azioni, siano in violazione di legge, potrà incorrere nelle responsabilità civili o penali previste.

10. GESTIONE DELLE REGISTRAZIONI SULLA BASE DEL PRESENTE DOCUMENTO

È istituito il Registro delle violazioni dei dati come da Allegato A).

11. VALIDITA' E GESTIONE DEL PRESENTE DOCUMENTO

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