CITTÀ DI POMPEI
PATRIMONIO DELL'UMANITÀ

Data BreachPolicy

Procedura di notifica di violazione dei dati personali

INDICE

1. PREMESSA

Il Comune di Pompei, di seguito Ente, 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 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 all'Ente e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli 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 all'Ente 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 dei 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 legislazione vigente.

3. COS'È 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:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà del dipendente (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai

sistemi informatici con successiva divulgazione delle informazioni acquisite);

- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche;
- 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:

- i dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati Autorizzati);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dagli Autorizzati 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 ex art. 28 GDPR o di autonomo Titolare (di seguito genericamente denominati Responsabili esterni);

Quando nel seguito di questo documento ci si riferirà ad entrambe queste categorie di soggetti, genericamente si indicheranno come "Destinatari".

Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e 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:

- dati personali trattati "da "e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo e con qualsiasi sistema aziendale.

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 Titolare del trattamento o un suo delegato mediante la compilazione dell'Allegato – Modulo di comunicazione interna di Data Breach da inviare a mezzo mail al Titolare all'indirizzo protocollo@pec.comune.pompei.na.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 – Modulo di comunicazione interna di Data Breach**, 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 la supervisione 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 l'Amministratore di Sistema o un suo delegato in caso di assenza.

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato
Modulo di comunicazione interna di Data Breach, 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 e con la supervisione del 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).

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, l'Ente dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza sulla base delle indicazioni e dei modelli presenti sul sito del Garante nazionale per la protezione dei dati www.garanteprivacy.it. Nel caso non si rispettasse il limite delle 72 ore, andrà motivato il motivo di tale ritardo.

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Ente dovrà provvedervi, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare del trattamento o da un suo delegato 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 effettinegativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o un suo delegato con la supervisione del DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e-mail, SMS, 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 - Modulo di comunicazione interna di Data Breach**, l'Ente sarà tenuta a documentarlo.

Tale documentazione sarà affidata al Titolare del trattamento o ad un suo delegato e vi provvederà mediante la tenuta **dell'Allegato - 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 – Modulo di comunicazione interna di Data Breach

Qualora scopra un presunto Data Breach, è pregato di informare immediatamente il Titolare del trattamento, compilando la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo e-mail: protocollo@pec.comune.pompei.na.it

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

ALLEGATO – REGISTRO DEI DATA BREACH

Numero Violazione	Data Violazione	Natura della Violazione	Categoria di Interessati	Categoria di dati personali coinvolti	Numero approssimativo di registrazioni dati personali	Conseguenze della Violazione	Contromisure adottate	Notifica Autorità Garante Privacy (S/N)	Comunicazione ai soggetti interessati (S/N)
1									