Data Breach Policy
Procedura di notifica di violazione dei dati personali

INDICE

1. PREMESSE

Il Comune di Grosseto, ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuto a mantenere sicuri i dati personali e/o sensibili 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 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'Amministrazione di una sanzione amministrativa pecuniaria.

2. SCOPO

Lo scopo di questa procedura è quello di disegnare un flusso per la gestione delle violazioni dei dati personali e sensibili trattati dal Comune di Grosseto**,** in qualità di Titolare del trattamento.

3. TITOLARE E RESPONSABILE AL TRATTAMENTO DEI DATI

Il ruolo del Titolare del trattamento nel Comune di Grosseto è ricoperto dal Sindaco pro-tempore**.**

Il ruolo del Responsabile al trattamento dei dati è affidato a ciascun Dirigente per il Settore di competenza che ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in esse previsto, nonchè di eseguire le istruzioni impartite dal Titolare. Il Responsabile del Trattamento ha facoltà di nominare eventuali figure di **responsabili esterni** del trattamento e soggetti autorizzati dandone puntuale informazione al Titolare.

4. COS'È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è un'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 aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuendola al 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 aziendale;
- 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 aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

5. 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 quali:

• i lavoratori 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 (di seguito genericamente denominati Destinatari interni o incaricati al trattamento);

• qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Comune di Grosseto 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 Destinatari esterni);

di seguito, genericamente denominati "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.

6. A QUALI TIPI DI DATI SI RIFERISCONO QUESTE PROCEDURE

Queste procedure si riferiscono a:

• dati personali e/o sensibili trattati "da "e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;

• dati personali e/o sensibili conservati o trattati a mezzo di qualsiasi altro 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. Per «dati sensibili» si intendono quei "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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".*

7. GESTIONE COMUNICAZIONE DI DATA BREACHES

Le violazioni di dati personali sono gestite dal Responsabile del Trattamento e dal DPO (ove designato).
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 - e comunque entro 48 ore dal momento in cui ne viene a conoscenza - **informare dell'incidente il Responsabile dell'Ufficio** il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Responsabile del Trattamento e il DPO (ove designato) mediante la compilazione dell'**Allegato A – Modulo di comunicazione interna di Data Breach** da inviare a mezzo mail all'indirizzo databreach@comune.grosseto.it

8. 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 Responsabile del Trattamento e /o al DPO 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).

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Responsabile del Trattamento e/o il DPO (ove designato) **dovranno coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile 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 Responsabile del Trattamento e/o il DPO dovranno darne informazione al Titolare del trattamento e 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 Responsabile del Trattamento designato e/o il DPO (ove designato) 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

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, si dovrà provvedere, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza. Per la segnalazione all'Autorità Garante dovrà essere utilizzato il modulo **Allegato C - Violazione di dati personali: Modello di comunicazione al Garante**.

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati ai soggetti interessati, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento

(UE) 2016/679, il Titolare dovrà provvedervi entro 72 ore e comunque senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione il Responsabile del Trattamento e/o il DPO (ove designato) dovranno:
• comunicare il nome e i dati di contatto del Responsabile del Trattamento e/o del DPO;
• descrivere le probabili conseguenze della violazione dei dati personali;
• descrivere le misure adottate o di cui si propone l'adozione da parte di (...) 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 Responsabile del Trattamento e/o il DPO (ove designato), dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali email, 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, ciascun Responsabile del Trattamento sarà tenuto a documentarlo e ad informare il Titolare del trattamento, il DPO ed il Responsabile Unico.

Tale documentazione sarà affidata al Responsabile del Trattamento e/o al DPO (ove designato) o che, con l'ausilio del Responsabile IT (qualora la violazione riguardi dati contenuti in sistemi informatici), provvederanno alla registrazione della violazione sull'**Allegato D - Registro dei Data Breach**.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.