COMUNE DI CALENDASCO

PROCEDURA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI DI DATI PERSONALI

Sommario

1. Premessa

1.1 La presente policy è adottata da:

COMUNE DI CALENDASCO, con sede in 29010 Calendasco, Via G. Mazzini n. 4, codice fiscale 00216710335, in persona del legale rappresentante pro tempore, nella qualità di Titolare del trattamento (di seguito "**Titolare**" o "**Ente**").

1.2 La policy disciplina le modalità organizzative e procedurali da seguire in caso di incidenti di sicurezza e violazioni di dati personali ("data breach"), al fine di garantire una gestione tempestiva degli eventi e ridurre i rischi per i diritti e le libertà delle persone fisiche interessate.

1.3 Nel presente documento sono descritte le procedure che il personale dell'Ente è tenuto ad osservare per:

- rilevare e segnalare tempestivamente eventuali incidenti di sicurezza che possano comportare una violazione di dati personali;
- consentire la presa in carico e la valutazione dell'evento da parte dei soggetti organizzativamente competenti;
- permettere al Titolare del trattamento di adempiere, ove necessario, agli obblighi di notifica all'Autorità di controllo ai sensi dell'art. 33 del GDPR e di comunicazione agli interessati ai sensi dell'art. 34 del GDPR.

1.4 La presente policy si applica a tutti i soggetti che, a qualunque titolo, trattano dati personali nell'ambito delle attività istituzionali dell'Ente.

2. Contesto normativo e regolamentare

2.1 La presente procedura è adottata in conformità:

- al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR), con particolare riferimento agli artt. 33 e 34;
- al D. Lgs. 30 giugno 2003, n. 196, come modificato dal D. Lgs. 10 agosto 2018, n. 101;

2.2 La presente procedura tiene altresì conto degli orientamenti e delle Linee guida adottati dal Comitato europeo per la protezione dei dati (European Data Protection Board – EDPB), nonché dei provvedimenti e delle indicazioni operative emanate dall'Autorità Garante per la protezione dei dati personali in materia di gestione e notifica delle violazioni di dati personali.

3. Incidenti di sicurezza e violazioni di dati personali

3.1 Ai fini della presente procedura, per incidente di sicurezza si intende un evento – o una serie di eventi – di origine dolosa o accidentale, interno o esterno all'organizzazione, che

può comportare la compromissione dei dati detenuti dall'Ente, mettendo a rischio uno o più dei principi di sicurezza delle informazioni: riservatezza, integrità o disponibilità.

3.2 Un incidente di sicurezza può riguardare dati personali o altre informazioni trattate dall'Ente e può verificarsi, ad esempio, in seguito ad un attacco informatico, ad un comportamento umano illecito o accidentale, ad una catastrofe naturale o a un malfunzionamento hardware o software.

3.3 In particolare, si configura:

- una violazione della riservatezza, in caso di divulgazione o accesso ai dati non autorizzati o accidentali;
- una violazione dell'integrità, in caso di modifica non autorizzata o accidentale dei dati;
- una violazione della disponibilità, in caso di perdita o distruzione non autorizzate o accidentali di dati.

3.4 Ai sensi dell'art. 4, par. 1, punto 12), del GDPR, per violazione di dati personali (o "data breach") si intende una 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.

3.5 La violazione di dati personali costituisce una particolare tipologia di incidente di sicurezza che riguarda specificamente dati personali e che può determinare la perdita di riservatezza, integrità o disponibilità degli stessi.

3.6 Pertanto, mentre tutte le violazioni di dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza costituiscono necessariamente una violazione di dati personali.

Figura 1 – Una violazione di dati personali è un particolare tipo di incidente di sicurezza che causa perdita di riservatezza, integrità o disponibilità di dati personali.

4. Violazione della disponibilità dei dati personali

4.1 Nell'ambito delle violazioni di dati personali, la compromissione della disponibilità può risultare meno immediatamente evidente rispetto alle violazioni di riservatezza o di integrità.

4.2 Si configura una violazione della disponibilità quando i dati personali risultano distrutti, persi o comunque non accessibili per un determinato periodo di tempo.

4.3 Tale situazione può verificarsi, ad esempio:

- in caso di cancellazione accidentale dei dati da parte di personale autorizzato o non autorizzato;
- in caso di perdita della chiave di decifratura relativa a dati cifrati;
- in caso di malfunzionamenti hardware o software che impediscano l'accesso ai dati;
- a seguito di attacchi informatici (es. ransomware o denial of service) che rendano temporaneamente o permanentemente indisponibili i sistemi informativi.

4.4 La violazione della disponibilità può avere carattere temporaneo o permanente e deve essere oggetto di valutazione ai sensi della presente procedura al fine di accertare l'eventuale sussistenza di una violazione di dati personali.

5. Notifica della violazione all'Autorità di controllo

5.1 Ai sensi dell'art. 33, par. 1, del GDPR, qualora una violazione di dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, l'Ente provvede a notificarla al Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

5.2 L'Ente si considera "a conoscenza della violazione" nel momento in cui è ragionevolmente certo che si sia verificato un incidente di sicurezza che ha comportato la compromissione di dati personali.

5.3 La decisione in merito alla necessità di procedere alla notifica è assunta all'esito della valutazione del rischio per i diritti e le libertà delle persone fisiche effettuata secondo le modalità previste dalla presente procedura.

5.4 Qualora la notifica non sia effettuata entro il termine di 72 ore, essa è comunque trasmessa senza ingiustificato ritardo ed è accompagnata da una motivazione del ritardo.

5.5 La notifica all'Autorità di controllo contiene almeno le informazioni previste dall'art. 33, par. 3, del GDPR e può essere effettuata anche per fasi successive qualora non sia possibile fornire tutte le informazioni contestualmente.

5.6 L'Ente documenta in ogni caso qualsiasi violazione di dati personali verificatasi, anche qualora la stessa non sia soggetta a notifica all'Autorità di controllo, al fine di consentire la verifica del rispetto degli obblighi previsti dall'art. 33 del GDPR.

Figura 1 – Tra gli indicenti di sicurezza che causano perdita di riservatezza, integrità o disponibilità di dati personali, vanno notificati al Garante per la protezione dei dati personali solo quelli dove risulta non improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

6. Comunicazione della violazione di dati personali agli interessati

6.1 Qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Ente provvede a comunicare la violazione agli interessati senza ingiustificato ritardo, ai sensi dell'art. 34 del GDPR.

6.2 La decisione in merito alla necessità di procedere alla comunicazione è assunta all'esito della valutazione del rischio effettuata secondo le modalità previste dalla presente procedura.

6.3 La comunicazione agli interessati è redatta in linguaggio chiaro e semplice e contiene almeno:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- la descrizione delle probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e, se del caso, per attenuarne i possibili effetti negativi.

6.4 Ove opportuno, la comunicazione può contenere indicazioni utili agli interessati per mitigare le possibili conseguenze della violazione, in relazione alla tipologia di dati coinvolti e al contesto del trattamento (ad es. attenzione all'utilizzo di dati personali pubblicati indebitamente, verifica di comunicazioni ricevute da terzi, contatto con l'ufficio competente per eventuali rettifiche o aggiornamenti).

6.5 La comunicazione è effettuata direttamente agli interessati mediante i canali di contatto disponibili (ad es. posta elettronica, PEC, comunicazione postale), salvo che ciò richieda

uno sforzo sproporzionato. 6.6 In tali casi, l'Ente procede mediante comunicazione pubblica o altra misura equivalente idonea a informare gli interessati con analoga efficacia.

6.7 La comunicazione relativa alla violazione è trasmessa separatamente da altre comunicazioni istituzionali, al fine di garantirne la chiarezza e l'immediata comprensibilità.

6.8 La comunicazione della violazione agli interessati non è richiesta qualora sia soddisfatta almeno una delle seguenti condizioni, ai sensi dell'art. 34, par. 3, del GDPR:

- l'Ente ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure sono state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi (quali, ad esempio, la cifratura);
- l'Ente ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richiederebbe sforzi sproporzionati (in tali casi l'Ente procede mediante una comunicazione pubblica o misura equivalente, idonea a informare gli interessati con analoga efficacia).

Figura 3 – Tra gli indicenti di sicurezza che causano perdita di riservatezza, integrità o disponibilità di dati personali, vanno comunicati alle persone fisiche coinvolte solo quelli che presentano un rischio elevato per i diritti e le libertà di queste ultime.

7. Valutazione del rischio per i diritti e le libertà delle persone fisiche

7.1 A seguito dell'accertamento di una violazione di dati personali, l'Ente effettua una valutazione del rischio per i diritti e le libertà delle persone fisiche interessate, al fine di determinare:

- la necessità di notificare la violazione all'Autorità di controllo ai sensi dell'art. 33 GDPR;

- la necessità di comunicarla agli interessati ai sensi dell'art. 34 GDPR.

7.2 Il rischio sussiste quando la violazione è suscettibile di comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati personali sono stati oggetto di compromissione.

7.3 Ai sensi del Considerando 85 del GDPR, tali danni possono includere, a titolo esemplificativo: discriminazione, furto o usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza di dati personali protetti da segreto professionale o qualsiasi altro significativo svantaggio economico o sociale.

7.4 La valutazione del rischio, effettuata dal Titolare del trattamento in attuazione del principio di responsabilizzazione, tiene conto della probabilità e della gravità dell'impatto sui diritti e sulle libertà degli interessati, considerando, ove pertinenti, i seguenti elementi:

- la tipologia di violazione (riservatezza, integrità o disponibilità);
- la natura e la sensibilità dei dati personali coinvolti;
- il volume dei dati e il numero degli interessati coinvolti;
- la facilità di identificazione degli interessati;
- la gravità delle possibili conseguenze per le persone fisiche;
- le caratteristiche particolari degli interessati (es. minori, soggetti vulnerabili);
- le caratteristiche del trattamento e del contesto in cui è avvenuta la violazione;
- l'eventuale adozione di misure tecniche di protezione (es. cifratura, pseudonimizzazione).

7.5 In alcuni casi, all'esito della valutazione di cui sopra, la violazione può essere ritenuta improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche e, pertanto, non soggetta all'obbligo di notifica all'Autorità di controllo. Ciò può avvenire, ad esempio:

- quando i dati oggetto della violazione risultino efficacemente protetti mediante tecniche di cifratura o altre misure che li rendano incomprensibili a soggetti non autorizzati;
- quando sia disponibile un backup integro e sia possibile il tempestivo ripristino dei dati senza impatti significativi sugli interessati.

8. Team per la gestione dei data breach

8.1 In caso di violazione di dati personali, la gestione dell'incidente è affidata al Titolare del trattamento, per il tramite del Legale Rappresentante o di un soggetto da questi delegato.

8.2 In relazione alla natura e alla gravità dell'incidente, possono essere coinvolti:

- il responsabile dell'ufficio interessato;
- il referente ICT o altro personale tecnico interno o esterno;
- eventuali ulteriori strutture organizzative competenti.

8.3 Il Responsabile della protezione dei dati personali (DPO) è tempestivamente informato della violazione e fornisce supporto e consulenza nella valutazione del rischio e nell'individuazione delle misure da adottare, ai sensi degli artt. 33 e 34 GDPR.

9. Gestione della violazione: rilevazione e valutazione preliminare

9.1 La scoperta di un incidente di sicurezza comportante un possibile data breach può derivare da:

- una segnalazione esterna (es. utente, fornitore, altra amministrazione);
- una rilevazione interna (es. dipendente o collaboratore).

9.2 È fondamentale che dipendenti e collaboratori segnalino immediatamente l'incidente al proprio responsabile gerarchico o al referente individuato dall'Ente per la gestione degli incidenti di sicurezza, che ne cura la tempestiva trasmissione al soggetto delegato dal Titolare. Il DPO è informato senza ritardo.

9.3 Il soggetto delegato dal Titolare, con il supporto del referente ICT o del responsabile dell'ufficio competente, raccoglie le informazioni utili per stabilire se vi sia stata una violazione di dati personali e per qualificarne la tipologia.

9.4 Ai fini dell'applicazione dell'art. 33 GDPR, il Titolare del trattamento si considera venuto a conoscenza della violazione nel momento in cui, a seguito della segnalazione interna o esterna, è ragionevolmente certo che si sia verificato un incidente di sicurezza che ha comportato la compromissione di dati personali. Da tale momento decorre il termine di 72 ore previsto per l'eventuale notifica al Garante per la protezione dei dati personali.

10. Gestione della violazione: contromisure e valutazione del rischio

10.1 Se, a seguito della valutazione preliminare, viene accertato che l'incidente ha comportato la perdita o la compromissione di dati personali, la gestione passa alla fase di analisi e contenimento dell'evento.

10.2 In questa fase:

- è confermata formalmente l'avvenuta violazione di dati personali;
- sono definite e attuate le contromisure tecniche e organizzative per limitare i danni e prevenire ulteriori violazioni;

- è effettuata la valutazione del rischio per i diritti e le libertà degli interessati;
- il soggetto delegato dal Titolare, tenuto conto anche del parere del DPO, decide in merito all'eventuale notifica al Garante per la protezione dei dati personali (art. 33 GDPR) e alla comunicazione agli interessati (art. 34 GDPR);
- l'evento è registrato nel registro interno delle violazioni di dati personali.

10.3 Le azioni intraprese variano in base all'esito della valutazione del rischio.

11. Gestione della violazione: notifica al Garante

11.1 Non tutte le violazioni di dati personali comportano l'obbligo di notifica al Garante per la protezione dei dati personali.

11.2 La notifica è richiesta qualora, a seguito della valutazione del rischio, non possa ritenersi improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche interessate (art. 33 GDPR).

11.3 Pertanto:

- se la violazione è ritenuta improbabile rispetto a tali rischi, l'evento è documentato nel registro interno delle violazioni di dati personali;
- se la violazione non è improbabile, il soggetto delegato dal Titolare provvede alla notifica al Garante per la protezione dei dati personali entro i termini previsti dalla normativa vigente.

12. Gestione della violazione: comunicazione agli interessati

12.1 Se la valutazione del rischio evidenzia un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, il soggetto delegato dal Titolare provvede alla comunicazione della violazione agli interessati senza ingiustificato ritardo, ai sensi dell'art. 34 GDPR.

13. Registro degli incidenti di sicurezza / violazioni di dati personali

13.1 Ogni violazione di dati personali è documentata, a prescindere dall'obbligo di notifica al Garante o di comunicazione agli interessati.

13.2 Il registro interno delle violazioni di dati personali contiene almeno:

- la natura della violazione e la data dell'evento;
- le circostanze in cui si è verificata;
- i provvedimenti adottati;

> le conseguenze accertate.

13.3 Le informazioni e la documentazione di supporto sono conservate in conformità ai criteri di conservazione stabiliti dalla normativa vigente e dalle policy interne dell'Ente.

12. Revisione e aggiornamento

12.1 Il presente documento può essere revisionato e aggiornato in relazione a mutamenti normativi o organizzativi dell'Ente.

13. Disposizioni finali

13.1 L'Ente provvede alla diffusione del presente documento con le modalità ritenute più opportune.