– Città di Montebelluna –

PROTOCOLLO
PER LA GESTIONE DELLE
VIOLAZIONI DI DATI PERSONALI

Aggiornato al 07.08.2024

Approvato con deliberazione di Giunta comunale n. 109 del 26.08.2024

SOMMARIO

1. Oggetto

Il presente protocollo individua gli indirizzi operativi da seguire per la valutazione della gravità delle violazioni di dati personali verificatesi nell'organizzazione del Titolare, al fine di valutare la necessità di provvedere alla notificazione all'Autorità Garante per la Protezione dei Dati Personali (AGPDP) o la comunicazione agli interessati ai sensi degli articoli 33 e 34 del reg. UE 2016/679 (GDPR).

2. Nozione di violazione

Ai sensi dell'art. 4, n. 12) GDPR si definisce "violazione di dati" *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,* dove per:

- **distruzione** si indicano le fattispecie nelle quali i dati personali non esistono più o non sono più disponibili in forme utilizzabili;
- **perdita** si intendono le fattispecie in cui il titolare ha perso il controllo sui dati personali che risultano non più disponibili anche per periodi di tempo limitato (**perdita temporanea**). Ovviamente non assume rilievo, ai fini della disciplina in materia di *Data Breach*, l'indisponibilità temporanea dei dati derivante ad es. dalla manutenzione periodica programmata dei sistemi IT del titolare;
- **modifica** si intende l'alterazione dei dati personali;
- **divulgazione non autorizzata o accesso** si intendono i casi di conoscenza/apprensione dei dati personali da parte di soggetti non autorizzati.

Le violazioni di dati personali possono riguardare, singolarmente o congiuntamente:

- **la riservatezza dei dati**, qualora consista nella divulgazione o nell'accesso non autorizzato o accidentale ai dati personali (es. violazione di sistemi o archivi da cui derivi il furto di dati personali, furto di credenziali, invio accidentale di un documento contenente dati personali ad un destinatario errato, la perdita di un supporto di memorizzazione contenente dati personali);
- **l'integrità dei dati**, qualora consista nell'alterazione non autorizzata o accidentale dei dati personali trattati (es. modifiche involontarie ad una base dati, alterazione dolosa del contenuto di un archivio);
- **la disponibilità dei dati,** qualora consista in un incidente che impedisca, temporaneamente o permanentemente l'accesso ai dati personali (es. distruzione degli archivi, cancellazione dolosa o colposa dei dati, temporaneo malfunzionamento dei sistemi (es. temporanea impossibilità di connettersi ad un archivio remoto).

La violazione può essere causata sia da incidenti di sicurezza che hanno ad oggetto i sistemi informativi del Titolare del trattamento (es. attacco hacker, guasto dei server, perdita di dispositivi di archiviazione portatili), sia non informatici (es perdita di documenti cartacei, intrusione nei locali del titolare e sottrazione non autorizzata di documenti).
La nozione di violazione di dati personali è dunque **particolarmente ampia ed onnicomprensiva.**

Secondo le linee guida elaborate dall'*Article 29 Data Protection Working Party*[1] sono qualificabili come violazioni di dati personali, ad esempio:

[1] Art. 29 WP, Guidelines 9/2022 on *Personal data breach notification under GDPR*, adottate il 10 ottobre 2022 e aggiornate il 28 marzo 2023 e Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione di dati personali.

- l'impossibilità di accedere ai dati delle pratiche o ai documenti dei fascicoli per un periodo significativo (perdita della disponibilità);
- una infezione di un *malaware* di tipo ransomware che cifri il contenuto di un computer contenente dati personali, rendendoli inaccessibili (perdita della disponibilità);
- una violazione dei sistemi informatici che comporti l'esfiltrazione dei dati ivi conservati (perdita della riservatezza);
- l'invio al destinatario errato di una e-mail contenente dati personali di altro interessato (perdita della riservatezza)
- la perdita o il furto di un dispositivo di archiviazione portatile o di un PC od altro dispositivo mobile contenente dati personali (perdita della riservatezza / disponibilità)
- la perdita o il furto di fascicoli cartacei (perdita della disponibilità/della riservatezza), contenenti dati comuni o particolari;
- la distruzione accidentale di documenti o l'alterazione del contenuto di documenti contenenti dati personali (perdita dell'integrità/disponibilità)
- l'inserimento errato di documenti nel fascicolo di una diversa pratica, se da ciò deriva la perdita della disponibilità del documento per un tempo apprezzabile;
- l'accesso da parte di persone non autorizzate ai fascicoli (perdita della riservatezza);
- attacchi di ingegneria sociale che portino alla compromissione dei sistemi o alla comunicazione di dati personali a soggetti non autorizzati (perdita della riservatezza).

3. Rilevazione della violazione e notifica

Ai sensi dell'art. 33 GDPR, il Titolare è tenuto a notificare all'Autorità di Controllo ogni violazione di dati che possa determinare un rischio per i diritti e le libertà delle persone fisiche **senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.** In caso di segnalazione oltre il suddetto termine il Titolare è tenuto a **giustificare il ritardo.** È dunque fondamentale l'adozione di procedure interne per la segnalazione e la tempestiva valutazione delle conseguenze della violazione.

4. Organizzazione interna del Titolare

Nell'ambito della propria organizzazione interna, il Comune di Montebelluna ha costituito un Gruppo di Lavoro Privacy, composto dal Segretario Comunale, dal Responsabile del Servizio informatico comunale, da un componente dell'Ufficio legale ed integrato da Responsabili di Settore, secondo le rispettive competenze, nonché dal Responsabile della Protezione dei Dati. Il Gruppo di Lavoro Privacy

sovrintende alla conformità dell'Amministrazione alla normativa in materia di protezione dei dati personali e svolge un ruolo di impulso e coordinamento dell'attività dei Settori.

Ciascun Responsabile di Settore ha ricevuto una delega di funzioni ai sensi dell'art. 2-quaterdecies d.lgs. n. 196/2003, per lo svolgimento di alcune attività connesse all'ottemperanza alla normativa in materia di protezione dei dati personali. Tra le funzioni delegate, i Responsabili di Settore hanno anche quella connessa alla raccolta delle segnalazioni di potenziali violazioni di dati ed alla loro tempestiva comunicazione al Titolare, per l'adozione dei conseguenti adempimenti.

In tale veste, i dirigenti di ciascun Settore assumono la veste di *Referente Privacy* nei confronti del personale comunale assegnato agli uffici ricompresi nel Settore di competenza.

I Referenti Privacy svolgono un ruolo di contatto con il Gruppo di Lavoro Privacy, al quale sono affidate funzioni di supporto al Titolare del trattamento nella gestione delle violazioni di dati.

5. Linee guida per la gestione delle violazioni

Di seguito sono esposte le linee guida da osservare nella gestione delle violazioni di dati personali. Le linee guida sono orientate al perseguimento dei seguenti obiettivi:

- dare risposta tempestiva alla violazione, allo scopo di mitigarne gli effetti negativi per gli interessati;
- tempestiva valutazione della portata e delle conseguenze della violazione, allo scopo di ottemperare agli obblighi di notifica/comunicazione delle violazioni nei termini previsti dalla legge;
- efficace adozione di misure correttive e vigilanza sulla loro implementazione ed efficacia.

A. Segnalazione della violazione – Tempo 0-1 h

Chiunque nell'organizzazione del Titolare abbia il ragionevole sospetto che si sia verificata una violazione dei dati personali trattati dal Titolare è tenuto a dare tempestivo avviso al proprio Responsabile di Settore, attraverso un canale di comunicazione scritto (es. e-mail).

La segnalazione deve contenere:

1) l'identificazione della persona che segnala la violazione;
2) gli uffici ed i servizi interessati dalla violazione;

3) i fatti che si sospettano costituire la violazione dei dati personali;
4) se noto, la data e l'ora in cui si è verificata la violazione e la sua durata
5) se noto, i dati che potrebbero essere stati oggetto di violazione;
6) se noto, le possibili conseguenze della violazione per gli interessati.

Il Referente Privacy, se non ritiene la segnalazione manifestamente infondata, informa senza ritardo il Delegato Privacy ed il DPO, con comunicazione scritta.

B. Accertamento dei fatti. Misure di mitigazione. – Tempo 2-36 h

Il Gruppo di Lavoro Privacy, con la collaborazione del personale di supporto e dei referenti delle sedi/aree di attività coinvolte nella violazione e, se opportuno, con il coinvolgimento dei responsabili IT e degli Amministratori di Sistema, procede ad acquisire ulteriori informazioni sui fatti oggetto di segnalazione, volti a confermare l'esistenza della violazione ed acquisire gli elementi utili al fine della stima della gravità della violazione.

Il Gruppo di Lavoro Privacy, valutata la segnalazione, informa senza ritardo il Sindaco, quale legale rappresentante del titolare. Agli incontri del Gruppo di Lavoro Privacy partecipa, in tutte le successive fasi, il Sindaco o altro membro della Giunta da lui delegato.

Sulla base degli elementi raccolti, il Gruppo di Lavoro Privacy, individuerà le misure che possono essere adottate per mitigare gli effetti della violazione quali, ad esempio:

- **nel caso di violazioni legate alla riservatezza,** la possibilità di distruggere i dati involontariamente o dolosamente diffusi o sottratti (es. richiesta di distruzione delle copie involontariamente diffuse, cancellazione a distanza dei dati contenuti in dispositivi smarriti o rubati, blocco immediato dei profili utente violati);
- **nel caso di violazioni connesse all'integrità,** la possibilità di ripristinare i dati danneggiati (es. ripristino di copie di sicurezza, ricostruzione delle basi dati da altri archivi, procedure di annullamento delle ultime modifiche apportate);
- **nel caso di violazioni connesse alla disponibilità,** la possibilità di ripristinare l'accesso ai dati (es. procedure di disaster recovery, recupero di backup, attivazione di sistemi ridondati, attivazione di connessioni alternative).

Le misure di mitigazione dovranno essere implementate nel minor tempo possibile.

C. Valutazione del rischio e delle conseguenze per gli interessati – Tempo 37-50 h

Completata l'istruttoria preliminare, il Gruppo di Lavoro Privacy, con il supporto del DPO procede alla valutazione delle possibili conseguenze della violazione per i diritti

e le libertà degli interessati, al fine di determinare se la violazione sia di gravità tale da richiedere la notifica all'Autorità di Controllo o la comunicazione agli Interessati.

Ai sensi dell'art. 33 GDPR, il titolare deve notificare il *Data Breach* all'autorità di controllo, "*a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*". Ad esempio, viene considerato improbabile che sussista un tale rischio nell'ipotesi di smarrimento di una chiavetta USB dotata di un sistema di criptaggio dei dati tale da renderli inaccessibili a terzi secondo i più elevati standard di sicurezza. La notifica deve essere svolta senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare ne è venuto a conoscenza. Il titolare che effettui la notifica dopo 72 ore è tenuto a motivare le ragioni del ritardo.

Ai sensi dell'art. 34 GDPR, il titolare o il Responsabile devono comunicare senza ritardo il *Data Breach* al soggetto o ai soggetti interessati "*quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche*". Ad esempio, un rischio elevato sussiste quando, in considerazione della tipologia di dati oggetto di violazione, l'interessato possa subire: discriminazioni e umiliazioni, furti di identità, frodi, perdite economiche o finanziarie, danni reputazionali.

Il rischio si considera particolarmente grave quando riguarda categorie di soggetti vulnerabili (es. minori, persone economicamente o socialmente deboli).

Il rischio per gli interessati è determinato sulla base di due elementi:

- **la gravità,** definita come il grado di afflizione ai diritti e le libertà degli interessati che la violazione è in grado di produrre (es. furti di identità, perdite patrimoniali, lesione dell'immagine e della reputazione, divulgazione di dati sensibili);
- **la probabilità**, definita come il grado di possibilità che si verifichino gli eventi temuti.

A questo fine, possono essere presi in considerazione elementi quali:

- la natura dei dati;
- il volume dei dati ed numero di interessati coinvolti;
- la facilità di identificazione degli interessati;
- l'appartenenza degli interessati a categorie vulnerabili (es. disabili, minori);
- la gravità delle potenziali conseguenze sui diritti e le libertà degli interessati;

Sulla base delle risultanze della valutazione si dovrà procedere alla notifica o comunicazione della violazione e dovranno essere definite le ulteriori misure che si ritenessero necessarie per limitare gli effetti della violazione.

Al fine di stimare la violazione è possibile ricorrere ad una griglia a doppia scala:

Gravità	**Basso**: la violazione non può generare alcun impatto (es. i dati riguardano esclusivamente persone giuridiche, i dati sono pseudonimizzati e non sono sufficienti a identificare gli interessati, i dati sono crittografati e non sono accessibili) **Medio-basso**: l'impatto potenziale è di scarsa gravità e reversibile (es. si tratta di dati comuni o la cui divulgazione o perdita non determina pregiudizi significativi in capo all'interessato) **Medio-alto:** l'impatto potenziale può essere significativo, ma non impattare diritti e libertà fondamentali o pregiudizi irreversibili **Alto**: impatto significativo ed irreversibile
Probabilità	**Improbabile:** il rischio non si è ancora verificato ed è improbabile che si verifichi. **Basso**: il rischio non si è ancora verificato e vi è una scarsa probabilità che si verifichi **Medio**: il rischio non si è ancora verificato ma potrebbe verificarsi **Alto**: il rischio si è già verificato

L'individuazione delle misure da adottare sarà così effettuata

TABELLA DI VALUTAZIONE					
		PROBABILITÀ			
GRAVITÀ		I	B	M	A
	B	Notifica: NO Comunicazione: NO	Notifica: NO Comunicazione: NO	Notifica: NO Comunicazione: NO	Notifica: SI Comunicazione: NO
	M/B	Notifica: NO Comunicazione: NO	Notifica: SI Comunicazione: NO	Notifica: SI Comunicazione: NO	Notifica: SI Comunicazione: SI
	M/A	Notifica: NO Comunicazione: NO	Notifica: SI Comunicazione: NO	Notifica: SI Comunicazione: SI	Notifica: SI Comunicazione: SI
	A	Notifica: NO Comunicazione: NO	Notifica: SI Comunicazione: NO	Notifica: SI Comunicazione: SI	Notifica: SI Comunicazione: SI

TABELLA DI VALUTAZIONE - ESEMPI					
	PROBABILITÀ				
GRAVITÀ		I	B	M	A
	B	Furto/Smarrimento di dispositivo elettronico contenente dati comuni crittografati	Furto di un supporto non crittato contenente dati personali generici (es. indirizzario)	Invio al destinatario errato di un messaggio di posta elettronica contenente dati comuni (es. generalità, indirizzo email) o sensibili di un numero ristretto di interessati	Esfiltrazione di dati dell'Amministrazione da parte di un funzionario.
	M/B	Furto di un dispositivo informatico contenente dati finanziari/giudiziari, la cui memoria è stata eliminata da remoto entro due ore dal furto	Smarrimento di documenti o dispositivi contenenti dati comuni, quando sia probabile che i documenti o il dispositivo siano andati distrutti e vi sia backup	Invio al destinatario errato di un messaggio di posta elettronica contenente dati particolari	Attacco ransomware che renda indisponibili i dati di una quota rilevante dei cittadini, con backup e senza esfiltrazione
	M/A	Furto di un dispositivo informatico contenente dati appartenenti a particolari categorie, la cui memoria è stata eliminata da remoto entro due ore dal furto	Furto di un dispositivo informatico contenente dati finanziari/giudiziari, la cui memoria è stata eliminata da remoto a dodici ore dal furto	Violazione di un profilo utente dotato di privilegi di accesso a dati finanziari o sensibili scoperto ad oltre 24 ore dall'evento	Violazione di un sistema e furto di una base dati contenente dati sensibili o finanziari
	A	Violazione dei sistemi informatici, che sia stata prontamente rilevata e bloccata, prima che l'attaccante potesse eseguire operazioni sui dati	Furto di supporti/fascicoli cartacei contenenti dati personali comuni non cifrati	Furto di supporti/fascicoli cartacei contenenti dati personali particolari non cifrati	Attacco ransomware con esfiltrazione che determina la mancanza di disponibilità dei dati per oltre ventiquattro ore

D. Notificazione, comunicazione e registrazione (Tempo 50-72 h)

1. Notificazione al garante

Nel caso in cui dalla valutazione sia emersa la necessità di procedere alla notificazione della violazione all'Autorità di Controllo, si dovrà procedere alla trasmissione, della notifica contenente tutti gli elementi previsti dall'art. 33 GDPR, secondo il modello approvato dall'Autorità Garante per la Protezione dei Dati Personali con provvedimento del 30 luglio 2019 (allegato al presente protocollo):

- una descrizione della natura della violazione dei dati personali, che comprenda, se possibile:
  - le categorie e il numero approssimativo di persone interessate;
  - le categorie e il volume approssimativo di dati personali interessati;
- il nome e i riferimenti di contatto del DPO;
- una descrizione delle possibili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi (v. §B);
- **in caso di notifica effettuata oltre il termine prescritto di 72 ore**, una descrizione dei motivi del ritardo.

La notifica va trasmessa all'AGPDP a mezzo pec all'indirizzo: **protocollo@pec.gpdp.it**

2. Comunicazione agli interessati (Tempo 50-72 h)

Qualora la valutazione abbia evidenziato la necessità di procedere alla comunicazione all'interessato, si dovrà verificare che non sussistano le ulteriori circostanze che, ai sensi dell'art. 34 GDPR, consentono di non effettuare la comunicazione:

a) se le misure tecniche e organizzative adottate dal titolare 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) se le misure adottate dal Titolare successivamente alla scoperta della violazione sono state idonee a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) se la comunicazione individuale a tutti gli interessati 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.

La comunicazione individuale, inviata ai recapiti noti dell'interessato (es. e-mail, pec, indirizzo postale). Devono essere preferiti contatti personali e diretti. La comunicazione tramite canali pubblici può avvenire in alternativa a quella sui canali personali qualora i canali personali non siano disponibili (ad es. il titolare non dispone di indirizzi email) oppure qualora la comunicazione personale richieda uno sforzo eccessivo al titolare.

La comunicazione deve contenere:

- il nome e i riferimenti di contatto del DPO;
- una descrizione delle possibili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi (v. §2).

3. Registrazione della violazione

In ogni caso, anche qualora non si proceda a notifica o comunicazione, il Delegato Privacy dovrà annotare la violazione nel registro delle violazioni predisposto dal Titolare.

La registrazione della violazione deve indicare:

- la descrizione della violazione;
- la data presunta della violazione;
- la data della scoperta;
- il luogo della violazione;
- l'indicazione della natura e la tipologia dei dati anche solo presumibilmente coinvolti;
- la descrizione degli strumenti di elaborazione o di memorizzazione dei dati coinvolti;
- l'indicazione delle categorie di interessati coinvolti ed il numero approssimativo di interessati coinvolti;
- l'indicazione del numero approssimativo di registrazioni di dati coinvolti;
- una descrizione delle probabili conseguenze della violazione dei dati personali
- una descrizione delle misure di mitigazione coinvolte;
- l'indicazione se è stata effettuata la notificazione al Garante o la comunicazione agli interessati e l'indicazione della data in cui tali adempimenti sono stati compiuti;

- nel caso in cui non siano state effettuate la notificazione o la comunicazione, una descrizione dei motivi per i quali è stato escluso di dover procedere a tali adempimenti;

E. Chiusura della procedura. *Follow up* e adeguamento.

Il Gruppo di Lavoro Privacy prosegue nel monitoraggio del *Data Breach* fino a quando vi è la ragionevole certezza che esso sia cessato e che si sia avuta contezza della sua estensione oggettiva e soggettiva.

Il Titolare del trattamento dovrà verificare la correttezza delle informazioni trasmesse all'Autorità di controllo ed agli interessati e trasmettere eventuali aggiornamenti rilevanti.

Le informazioni raccolte e le risultanze delle indagini svolte a seguito della violazione dovranno essere prese in considerazione nell'ambito delle procedure di adeguamento/revisione delle misure tecniche ed organizzative, al fine di evitare il ripetersi di violazioni analoghe a quella verificatasi.

A questo fine, dovrà essere predisposto un piano di verifica periodica dello stato di attuazione e dell'efficacia delle misure di mitigazione, organizzative e tecniche adottate.