



COMUNE DI NAGO-TORBOLE
PROVINCIA DI TRENTO

Circolare del Segretario comunale

Alla cortese attenzione
dei Dipendenti e degli Amministratori

Numero di protocollo associato al documento
come metadato (DPCM 3.12.2013, art. 20).
Verificare l'oggetto della PEC o i files allegati alla
medesima. Data di registrazione inclusa nella
segnatura di protocollo.

Oggetto: Aggiornamento della procedura di violazione dei dati personali (c.d. Data breach)

Si informa che con deliberazione della Giunta comunale n. 71 del 20 agosto 2026, esecutiva, è stata aggiornata la procedura per la gestione delle violazioni dei dati personali ("data breach"), originariamente adottata con deliberazione del 16 settembre 2019. L'aggiornamento riguarda, in particolare, le modalità operative di segnalazione e notifica delle violazioni dei dati personali al Garante per la protezione dei dati personali.

Si rammenta che la disciplina di riferimento è contenuta negli articoli 33 e 34 del Regolamento (UE) 2016/679 e nelle pertinenti Linee guida in materia di notifica delle violazioni dei dati personali (Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del GDPR e Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica di una violazione dei dati personali).

Per **data breach** si intende una violazione di sicurezza che comporta una violazione dei dati personali in termini di:

- violazioni della riservatezza, ossia disvelamento o accesso indebito o accidentale ai dati personali;
- violazioni della disponibilità, ossia indebito o accidentale impedimento all'accesso ai dati personali o distruzione di dati personali;
- violazione dell'integrità, ossia indebita o accidentale alterazione dei dati personali.

A seguire alcuni esempi di violazione:

1	Un addetto dell'ente smarrisce o subisce il furto di un dispositivo di memorizzazione (cd, dvd, hd esterno, pen drive) o di un dispositivo personale (pc, tablet, smartphone) contenenti dati personali non protetti da crittografia e non recuperabili dalle copie di backup. (Nel caso in cui i dati siano crittografati l'evento non è da considerare una violazione della riservatezza. Nel caso in cui siano disponibili copie di backup l'evento non è da considerare una violazione della disponibilità.)
---	---

2	A causa di un malware o di un virus informatico l'ente perde l'unica copia non recuperabile dal backup di un insieme di dati personali (database o cartelle).
3	A causa di un evento dannoso quale può essere un incendio o un allagamento l'ente perde alcune banche dati (originali cartacee o elettroniche senza possibilità di ripristino dalle copie di backup).
4	Il locale archivio dell'ente subisce una effrazione e il furto di alcuni faldoni contenenti dati personali.
5	Documenti contenenti dati personali sono stati smaltiti per errore in un cestino gettacarte anziché essere distrutti in modo sicuro. Il cestino è stato svuotato in un bidone lasciato all'esterno dell'ufficio ai fini della raccolta dei rifiuti. Un terzo ha prelevato la busta da quest'ultimo bidone e ha avuto accesso ai dati personali.
6	A seguito di un attacco informatico ad un servizio online dell'ente vengono prelevati e diffusi dati personali degli utenti.
7	Un dipendente ha rivelato ad un terzo il login e la password di un account con privilegi di accesso completo ad una o più basi dati dell'ente. Utilizzando tale account, il terzo può accedere a tutte le informazioni presenti nella base dati quali nomi, indirizzi, indirizzi di posta elettronica, numeri di telefono, dati di accesso e altri dati di identificazione (nome utente, hash delle password, ID dei clienti).
8	A seguito di un guasto, di una interruzione di corrente o della connettività si verifica una prolungata sospensione nell'erogazione dei servizi ai cittadini.
9	Un cittadino segnala di aver ricevuto per sbaglio documentazione contenente dati personali relativi ad altri soggetti.
10	Una e-mail contenente dati personali viene inviata per sbaglio ad un elevato numero di destinatari.

Chiunque venga a conoscenza di una possibile violazione dei dati personali è tenuto a segnalare immediatamente al Referente Data Breach, individuato nella Vicesegretaria comunale. L'omessa segnalazione può comportare responsabilità a carico del soggetto che, pur essendo a conoscenza dell'evento, non vi abbia provveduto.

In allegato la procedura completa per la violazione dei dati, comprensiva degli allegati.

Confidando nella massima collaborazione, si porgono cordiali saluti.

Il Segretario comunale
dott. Giorgio Osele



GIORGIO
OSELE
09.09
.2026
13:04:18
UTC