AZIENDA FORESTALE TRENTO – SOPRAMONTE

Azienda Speciale Consorziale

PEFC
PEFC/18-21-02/137

AFTS/2026/1.6-2026/NM
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. Negli esemplari cartacei segnatura di protocollo in alto a sinistra (da citare nella risposta).

Ai
Dipendenti e Amministratori
dell'Azienda forestale Trento - Sopramonte
a mezzo PiTre

Oggetto: Procedura di violazione dei dati personali (c.d. DATA BREACH).

La presente per comunicare l'aggiornamento della procedura di data breach, approvata con deliberazione della Commissione amministratrice n. 14 d.d. 3/3/2026 che disciplina l'iter da seguire in caso di violazione di dati personali.
I riferimenti normativi si rinvengono negli articoli 33 e 34 del Regolamento UE 679/2016 e nelle Linee guida del Gruppo "Articolo 29" in materia di notifica delle violazioni dei dati personali (Linee guida 9/2022 in materia di notifica delle violazioni di dati personali; Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica di violazione dei dati).
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.

1. Gestione interna del data breach seguendo l'apposita procedura adottata dall'Azienda

In caso di supposta violazione di dati personali deve essere avvisato tempestivamente il Referente Data breach (Direttore) e il Referente Privacy dell'Azienda (Direttore) affinchè:

- vengano adottate le Misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, venga informato immediatamente il Responsabile della Protezione dei Dati per una valutazione condivisa;
- venga condotta e documentata un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) attraverso la compilazione del

"Modello di potenziale violazione di dati personali al Responsabile Protezione Dati".

2. Notificazione data breach al Garante

In caso di violazione dei dati personali, previo consulto con il Responsabile della Protezione dei Dati, si deve notificare la violazione al Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui l'Azienda ne è venuta a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore dovrà essere documentato il motivo del ritardo. La notifica deve contenere una serie di elementi come indicati nella norma, e in particolare:

- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- nome e dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La notifica deve avvenire telematicamente attraverso il portale messo a disposizione dall'Autorità Garante al seguente link: https://servizi.gpdp.it/databreach/s/

3. Comunicazione data breach

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve comunicare la violazione all'interessato senza ingiustificato ritardo. In presenza di alcune condizioni non è necessaria la comunicazione all'interessato.

4. Registro delle violazioni

Deve essere formato un Registro delle violazioni i dati personali e, nel caso si verifichi un evento che comporti, o possa comportare, una violazione dei dati personali, oltre a quanto sopra indicato, andrà compilato il Registro con le informazioni necessarie a gestire l'evento, tra cui quanto occorso; gli elementi caratterizzanti il caso; le azioni e le misure migliorative da adottarsi.

5. Esempi di violazioni

	Violazione
1	Un addetto dell'Azienda 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 crittografazione 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'Azienda 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'Azienda perde alcune banche dati (originali cartacee o elettroniche senza possibilità di ripristino dalle copie di backup).
4	Il locale archivio dell'Azienda 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'Azienda 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'Azienda. 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.

6. Formazione

Al fine di riconoscere una violazione di dati personali e tutti gli adempimenti necessari per evitarla, è necessario che tutti i dipendenti e gli amministratori siano costantemente informati e formati in materia di protezione dati personali.

Distinti saluti.

Il Direttore
dott. Maurizio Fraizingher
(firmato digitalmente)

Questo documento, se trasmesso in forma cartacea costituisce copia dell'originale informatico firmato digitalmente predisposto e conservato presso questa Amministrazione in conformità alle regole tecniche (artt. 3 bis e 71 D.Lgs. 82/05). La firma autografa è sostituita dall'indicazione a stampa del nominativo del responsabile (art. 3 D. Lgs. 39/1993).

AZIENDA SPECIALE CONSORZIALE FORESTALE TRENTO - SOPRAMONTE
38122 TRENTO - Via del Maso Smalz, 3
Tel. 0461 889740 – Fax 0461 889741
E-mail: info@aziendaforestale.tn.it - Legal-mail: info@pec.aziendaforestale.tn.it
Codice fiscale 80016510226 - Partita IVA 00835990227