PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

DELL'AZIENDA FORESTALE TRENTO - SOPRAMONTE

Documento approvato con Deliberazione della Commissione amministratrice di data 10 dicembre 2020, n. 50		
Revisioni	Data	Motivo
1	Marzo 2026 (delibera Commissione amministratrice n. 14 del 3/3/2026)	Aggiornati i riferimenti del gruppo di lavoro Aggiornata con la nuova procedura dettata dall'Autorità Garante, che prevede dal 1° luglio 2021 la notifica tramite piattaforma messa a disposizione dalla medesima Autorità

INDICE

1 Scopo

Il presente documento contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016.

Tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente devono essere informati e osservare la presente Procedura.

2 Aggiornamento

Il Referente privacy dell'Ente, nel caso di variazioni organizzative e/o normative, aggiorna la presente procedura e la propone in approvazione alla Commissione amministratrice affinché la renda esecutiva.

3 Definizioni

Le seguenti definizioni dei termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento europeo n. 679 del 2016:
«**dato personale**»: 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;
«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
«violazione dei dati personali»: 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 in formato elettronico e/o cartaceo;
«**Responsabile della Protezione dei Dati**»: incaricato di assicurare la corretta gestione dei dati personali nell'Ente;
«Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE.

Nella presente procedura, per **«Ente»** si intende l'Azienda forestale Trento – Sopramonte.

4 Organizzazione delle attività di gestione dell'evento violazione dei dati personali

Il Titolare deve:

- designare un Referente della gestione delle violazioni dei dati personali (di seguito Referente data breach), figura che potrebbe coincidere con il Referente privacy dell'Ente. il Titolare può designare anche un gruppo di lavoro, denominato Gruppo di gestione delle violazioni dei dati personali, che supporta il Referente privacy e di cui lo stesso funge da coordinatore. Il Gruppo è formato da personale avente professionalità rilevanti in materia di trattamento di dati personali per i diversi profili di interesse (competenza informatica, legale, contrattualistica, ecc.);
- comunicare i nominativi del Referente privacy e del Referente data breach a tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente;
- nel caso di modifica/sostituzione dei soggetti preposti il titolare provvede a comunicare i nuovi nominativi a tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente;
- avvalendosi del Referente data breach, predisporre il Registro delle violazioni dei dati personali.

5 Gestione delle attività conseguenti ad una possibile violazione di dati personali

Il soggetto che, a diverso titolo o in quanto autorizzato al trattamento di dati personali di cui è titolare l'Ente, viene a conoscenza di una possibile violazione dei dati personali, deve immediatamente segnalare l'evento al Referente Privacy dell'Ente e al Referente data breach e fornire loro la massima collaborazione.
La mancata segnalazione del suddetto evento comporta a diverso titolo responsabilità a carico del soggetto che ne è a conoscenza.
Il Referente data breach deve:

- adottare le Misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, informare immediatamente il Responsabile della Protezione dei Dati per una valutazione condivisa;
- condurre e documentare 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";
- condividere con il Referente privacy e il Titolare i risultati dell'indagine;
- riferire i risultati dell'indagine al Responsabile della Protezione dei Dati inviando il "modello di potenziale violazione di dati personali al Responsabile Protezione Dati" compilato all'indirizzo serviziorpd@comunitrentini.it.

Il Responsabile della Protezione dei Dati, ricevuti i risultati dell'indagine, analizza l'accaduto e formula un parere in merito all'evento, esprimendo la propria valutazione, non vincolante, che lo stesso configuri in una violazione dei dati personali e che possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche.

6 Notifica della violazione dei dati personali all'Autorità Garante

Il Titolare, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, e dalle valutazioni fatte congiuntamente dal Referente della gestione delle violazioni dei dati personali e dal Referente Privacy dell'Ente, se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione avvalendosi della procedura telematica disponibile al seguente link: https://www.garanteprivacy.it/data-breach.
La notifica deve essere effettuata senza ingiustificato ritardo dall'accertamento dell'evento e, ove possibile, entro 72 ore dall'accertamento dello stesso con le modalità e i contenuti previsti dall'art. 33 del Regolamento europeo n. 679 del 2016.

7 Comunicazione della violazione dei dati personali agli interessati

Il Titolare, accertata la violazione dei dati personali e ritenendo che la stessa possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, oltre alla notifica di cui al punto 6, decide le modalità di comunicazione di tale violazione agli interessati, come previsto dall'art. 34 del Regolamento europeo n. 679 del 2016.

8 Compilazione del Registro delle violazioni dei dati personali

Il Titolare, avvalendosi del Referente data breach, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nel Registro delle violazioni dei dati personali.
Tale documento è tenuto e implementato dal Referente data breach e consente all'autorità di controllo di verificare il rispetto dall'art. 33 del Regolamento europeo n. 679 del 2016.

AZIENDA FORESTALE TRENTO – SOPRAMONTE

Azienda Speciale Consorziale

PEFC
PEFC/18-21-02/137

POTENZIALE VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL RESPONSABILE DELLA PROTEZIONE DEI DATI

Ente _____

Referente Privacy _____

Telefono _____ **Email** _____

Breve descrizione della violazione dei dati personali

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca di dati?

- Il _____
- Tra il _____ e il _____
- In un tempo non ancora determinato
- È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio: tipo di violazione

- Lettura (presumibilmente i dati non sono stati copiati)
- Copia (i dati sono ancora presenti sui sistemi del titolare)
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- Furto (i dati non sono più sui sistemi del titolare e non li ha l'autore della violazione)
- Altro _____

Dispositivo o strumento oggetto della violazione

- ❼ Computer
- ❼ Rete
- ❼ Dispositivo mobile
- ❼ File o parte di un file
- ❼ Strumento di backup
- ❼ Documento cartaceo
- ❼ Software _____
- ❼ Servizio informatico _____
- ❼ Altro _____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ❼ Numero _____ di persone
- ❼ Circa _____ persone
- ❼ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- ❼ Dati anagrafici/codice fiscale
- ❼ Dati di accesso e di identificazione (*username, password, customer ID, altro*)
- ❼ Dati relativi a minori
- ❼ 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
- ❼ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ❼ Dati giudiziari
- ❼ Copia per immagine su supporto informatico di documenti analogici
- ❼ Ancora sconosciuto
- ❼ Altro _____

Fornitori o soggetti esterni coinvolti

Misure tecniche, informatiche e organizzative applicate ai dati oggetto di violazione

Luogo e data _____

Firma _____

Registro delle violazioni dei dati dell'AZIENDA FORESTALE TRENTO – SOPRAMONTE								
NR.	**Data accadimento**	**Data comunicazione al referente interno**	**Breve descrizione evento**	**Servizio/Ufficio competente al trattamento**	**Coinvolgimento RPD: SI/NO**	**Azioni / Misure adottate**	**Notifica al Garante SI/NO e data**	**Comunicazione agli interessati SI/NO e data**
1								
2								
3								
4								
5								
6								