UNIVERSITÀ
DI TRENTO

Informativa sul trattamento dei dati personali nell'ambito dell'utilizzo della piattaforma Microsoft Defender for Endpoint

Il Regolamento UE 2016/679 "Regolamento Generale sulla protezione dei dati personali" (d'ora in avanti "GDPR") sancisce il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano.

Ai sensi degli artt. 13 del GDPR, l'Università degli Studi di Trento intende fornire a tutti gli utenti delle postazioni di lavoro di Ateneo (d'ora in avanti "interessati") le seguenti informazioni.

1. **Titolare del trattamento**

Il Titolare del trattamento è l'Università degli Studi di Trento, via Calepina n. 14, 38122 Trento (TN); email: ateneo@unitn.it.; ateneo@pec.unitn.it.

2. **Contatti del Responsabile della protezione dei dati**

Il **Responsabile della protezione dei dati (RPD),** al quale rivolgersi per informazioni relative ai propri dati personali, può essere contatto al seguente indirizzo email: **rpd@unitn.it**.

3. **Finalità del trattamento e base giuridica**

L'Università di Trento effettua il trattamento di dati personali nell'ambito dell'esecuzione dei propri compiti istituzionali (art. 6, par. 1, lett. e) del GDPR) esclusivamente per la finalità di implementare delle soluzioni, nell'ambito della cybersecurity e delle misure di sicurezza dei dati personali, che consentano di prevenire, rilevare, analizzare e rispondere alle minacce agli endpoint dell'organizzazione, quali le postazioni di lavoro.

La soluzione scelta dall'Ateneo è la piattaforma Microsoft Defender for Endpoint che garantisce, da una parte la sicurezza e l'integrità dalle postazioni di lavoro consentendo il rilevamento di attacchi avanzati quasi in tempo reale e dall'altra di assegnare priorità agli eventi di alert (ad esempio la presenza di un virus/malvare su una postazione) e intervenire da parte degli analisti della sicurezza in maniera efficace per prevenire/affrontare le eventuali minacce.

4. **Categorie dei dati trattati**

I dati raccolti sono prevalentemente anonimi e rientrano nella categoria dei metadati e dei dati di sistema, non sempre riconducibili ad una persona fisica:

- Informazioni sui files presenti nel sistema (dimensioni, nomi, hash)
- Dati riguardanti i processi attivi sul sistema
- Dati riguardanti le chiavi di registro del sistema

- Dati atti ad identificare univocamente il client quali serial numbers, versioni di sistema operativo, nome, software installato, ecc.
- Informazioni sulle connessioni di rete effettuate (indirizzi ip e porte)

5. Modalità di trattamento

Il trattamento dei dati personali viene effettuato mediante i tools di analisi messi a disposizione dalla piattaforma da parte di personale autorizzato al trattamento dei dati in relazione ai compiti e alle mansioni assegnate e nel rispetto dei principi di liceità, correttezza, trasparenza, adeguatezza, pertinenza, esattezza, non eccedenza, integrità e riservatezza (art. 5, par.1, GDPR).

La generazione degli eventi di alert avviene attraverso l'analisi automatizzata della postazione e per alcuni di questi eventi (es: rilevata la presenza di un software malevolo, Defender si attiva per eliminarlo o mettere in quarantena il file) ricorre ad azioni predefinite.

In particolare, a fronte di un evento di alert segnalato dalla piattaforma, l'analista della sicurezza incaricato potrà eseguire analisi approfondite per risolvere la problematica emersa e mettere in sicurezza le postazioni di lavoro coinvolte.

Al fine di garantire la sicurezza di tutte le postazioni di lavoro, l'analista di sicurezza potrà accedere a tutti i dati raccolti dalla piattaforma in modo da poter eventualmente indentificare problematiche di sicurezza non limitate alla sola postazione da cui è partito l'evento di alert (Threat Hunting).

Tutti i dati raccolti vengono salvati su sistemi cloud ospitati in Europa. Prima del salvataggio su supporto fisico, i dati vengono cifrati (encryption at rest). Tutti i protocolli di trasferimento dati (dalle postazioni di lavoro verso i sistemi cloud e viceversa) ne garantiscono sicurezza ed integrità (encryption in motion).

6. Periodo di conservazione dei dati

I dati raccolti saranno conservati per il periodo necessario alla realizzazione delle finalità sopraindicate ovvero per il tempo massimo previsto dal tool di analisi (180 giorni).

7. Diritti degli interessati

In ogni momento gli interessati potranno esercitare nei confronti del Titolare, ai contatti email sopraindicati, con riferimento ai dati personali ed esclusi i trattamenti dei dati di sistema e dei metadati, i diritti sanciti dagli artt. 15 e ss. del GDPR:

- **accesso ai propri dati personali** e alle altre informazioni indicate all'art. 15 del GDPR;
- **rettifica dei propri dati personali** qualora inesatti e/o la loro **integrazione** ove siano incompleti;

- **cancellazione** dei propri dati personali tranne i casi in cui l'Università sia tenuta alla loro conservazione ai sensi dell'art. 17, 3 par. lett. b) del GDPR;
- **limitazione del trattamento** nelle ipotesi indicate dall'art. 18 del GDPR;
- **opposizione al trattamento** dei dati personali che li riguardano nei casi in cui ciò sia consentito ai sensi dell'art. 21 del GDPR.

Per l'esercizio dei diritti è possibile utilizzare l'apposito modulo che si trova nella pagina "Privacy e protezione dei dati personali" del portale di Ateneo e inviarlo ai contatti sopraindicati del Titolare.

Gli interessati che ritengono che il trattamento dei loro dati personali avvenga in violazione del GDPR hanno diritto di proporre reclamo al Garante per la protezione dei dati personali ai sensi dell'art. 77 del GDPR o di adire le opportune sedi giudiziarie.