INFORMATIVA AI SENSI DEL REGOLAMENTO GENERALE PER LA PROTEZIONE DEI DATI – REGOLAMENTO UE 2016/679 E AL DECRETO LEGISLATIVO N. 196/2003 E S.M.I. "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" – TRATTAMENTO PER GESTIONE CENTRALIZZATA DELLE POSTAZIONI UTENTI (ENDPOINT) ATTRAVERSO L'USO DELLA SOLUZIONE CLOUD MICROSOFT INTUNE – Rif. Trattamento n. 23

Microsoft Intune è un servizio basato su tecnologia cloud Azure di Microsoft per la gestione di dispositivi mobili (MDM, Mobile Device Management) e per la gestione di applicazioni mobili (MAM, Mobile Application Management). Attraverso Intune è possibile gestire centralmente i dispositivi di proprietà dell'Ateneo, inclusi telefoni cellulari, tablet e calcolatori. È anche possibile configurare criteri specifici per la gestione centralizza delle applicazioni (es. aggiornamento, installazione ecc.)

Con Intune, è possibile:

- Impostare le regole e configurare le impostazioni nei dispositivi di proprietà dell'organizzazione per accedere ai dati e alle reti.
- Distribuire e autenticare le applicazioni nei dispositivi, in locale e nei dispositivi mobili.
- Proteggere le informazioni di Ateneo controllando il modo in cui gli utenti accedono alle informazioni e le condividono.
- Assicurarsi che i dispositivi e le applicazioni siano conformi ai requisiti di sicurezza e sempre aggiornati

I dati elaborati da Intune, noto anche come Endpoint Manager, verranno integrati nella soluzione antivirus e antimalware cloud "Microsoft Defender for Enpoint" per centralizzare la gestione della prevenzione e gestione degli attacchi informatici agli endpoint.

I dati all'interno della soluzione Intune sono trattati in conformità al Regolamento Generale per la Protezione dei Dati - Regolamento UE 2016/679 e al Decreto Legislativo n. 196/2003 e s.m.i. "Codice in materia di protezione dei dati personali" come novellato dal D.Lgs. 101/2018.
La presente informativa è resa, ai sensi Regolamento Generale per la Protezione dei Dati - Regolamento UE 2016/679.

1. **Titolare del Trattamento, Responsabile della protezione dei dati**
Il Titolare del Trattamento è l'Università degli Studi dell'Insubria, nella persona del Magnifico Rettore, con sede legale in Varese (VA) Via Ravasi, 2, pec ateneo@pec.uninsubria.it.
Gli Interessati possono rivolgersi al Responsabile della protezione dei dati per l'esercizio dei diritti previsti dal GDPR (artt. da 12 a 21) utilizzando il seguente indirizzo e-mail: privacy@uninsubria.it.
L'elenco aggiornato dei responsabili e degli autorizzati al trattamento è custodito presso la sede del Titolare del trattamento.

2. Oggetto del trattamento

- Dati utente (Nome del proprietario/nome visualizzato dell'utente - Nome dell'entità utente o indirizzo di posta elettronica - Numero di telefono - Identificatore dell'utente di terze parti (ad esempio ID Apple)
- Dati sull'inventario hardware (Nome del dispositivo - Produttore Sistema operativo - Numero di serie - Numero IMEI - Indirizzo IP - MacAddress Wi-Fi - ICCID) - Intune - Dati del log di controllo, compresi i dati sulle attività seguenti (Gestire - Creazione - Aggiornamento - Elimina - Assegnazione - Attività remote)
- Dati di supporto (Informazioni di contatto - Comunicazioni tramite posta elettronica con membri dei team Microsoft di supporto, del prodotto e/o dell'esperienza clienti)
- Dati sul controllo di accesso (Autenticatori statici, Chiavi di privacy per i certificati)
- Dati su amministratore e account (Nome e cognome dell'amministratore - Nome utente dell'amministratore - UPN - Numero di telefono - Indirizzo di posta elettronica del proprietario dell'account - ID di Active Directory di ogni amministratore IT del cliente - Dati di pagamento per la fatturazione del cliente - Chiave di sottoscrizione)
- Dati creati dall'amministratore, ad esempio Nomi di profilo Criteri di conformità Criteri di gruppo Script PowerShell Applicazione line-of-business (LOB)
- Dati inventario applicazioni (nome dell'app - Versione - ID dell'app - size - percorso di installazione -NB I dati di inventario dell'applicazione vengono raccolti solo quando contrassegnati dall'amministratore come dispositivo aziendale o quando è attivata la funzionalità per le app conformi.
- ID tenant di terze parti del cliente (ad esempio l'ID Apple)
- Dati del dispositivo (ID dispositivo Intune - ID dispositivo di Azure Active Directory - ID di gestione dei dispositivi in Intune - ID tenant - ID account - ID dispositivo EAS - ID specifici della piattaforma - ID Apple per dispositivi iOS/iPadOS - Indirizzo Mac per dispositivi Mac - ID Windows per dispositivi Windows
- Dati sulle applicazioni gestite (ID delle applicazioni gestite - Tag del dispositivo delle applicazioni gestite - ID di gestione dei dispositivi in Intune - ID dispositivo di Azure Active Directory - Chiavi di crittografia)
- Dati di utilizzo amministrativi da tutti i tenant di Intune (ad esempio, controlli amministrativi selezionati durante le interazioni con la console di amministrazione)
- Dati sull'account tenant (Numero di dispositivi o utenti registrati - Numero di piattaforme per dispositivi identificate - Numero di dispositivi installati - installedDeviceCount - notApplicableDeviceCount - notInstalledDeviceCount – pendingInstallDeviceCount
- Identificatore proattivo di attacco (IOAs) – indicatore, gestito all'interno del sistema defender per Endpoint per generare allerte e fornire indicazioni su possibili compromissioni di device, file e url in uso presso gli endpoint

La lista aggiornata dei dati raccolti è disponibile al seguente link
https://docs.microsoft.com/en-us/mem/intune/protect/privacy-data-collect
Microsoft Defender for Endpoint data storage and privacy | Microsoft Docs

In particolare, NON vengono mai raccolti dati per scopi di profilazione o marketing o dati relativi alle chiamate degli utenti, la navigazione internet, email personali, messaggi di testo, contatti, password personali, calendari di eventi o fotografie, incluse quelle presenti nelle app fotografiche installate o negli archivi personali di foto.

3. **Finalità del trattamento cui sono destinati i dati:**
   La finalità del trattamento è la tutela del patrimonio, la sicurezza e protezione dei dati e della rete di Ateneo, in particolare attraverso l'aggiornamento di sicurezza e funzionale del parco macchine di proprietà di Ateneo e la possibilità di un controllo condizionale nella gestione dei dati aziendali (es. cancellazione automatica da remoto in caso di furto, criptazione dei dischi con rotazione automatica delle chiavi di crittazione ecc.). Il trattamento migliora l'erogazione di servizi resi possibili attraverso i sistemi di automazione installati, gestiti e aggiornati centralmente attraverso la soluzione intune, la centralizzazione e remotizzazione degli interventi di helpdesk/servidesk per le postazioni di lavoro degli utenti (endpoint) e la rilevazione di telemetrie di funzionamento generale degli endpoint per identificare potenziali problemi di prestazioni prima che questi rappresentino una limitazione all'operatività della postazione.

4. **Base Giuridica dei Trattamenti**
   a) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
   b) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
   c) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

5. **Obbligatorietà o meno del conferimento dei dati**
   Il conferimento dei dati è obbligatorio per il funzionamento del sistema

6. **Modalità del trattamento**
   La raccolta dei dati avviene nel rispetto dei principi di liceità, correttezza, pertinenza, completezza e non eccedenza in relazione ai fini per i quali sono trattati. I dati personali sono trattati in osservanza dei principi di liceità, correttezza e trasparenza, previsti dalla legge, con l'ausilio di strumenti atti a registrare e memorizzare i dati stessi e comunque in modo tale da garantirne la sicurezza e tutelare la massima riservatezza dell'interessato.

7. **Periodo di conservazione dei dati**
   Il periodo di conservazione dei dati è di 30 giorni. I log di audit sono conservati un anno per ragioni di sicurezza. https://docs.microsoft.com/en-us/mem/intune/protect/privacy-data-store-process
   I dati utenti per il modulo "Endpoint Defender" sono conservati per 30 giorni in formato completo per permettere una analisi query-based per il thread-hunting. I dati dell'intero sistema Endpoint Defender saranno cancellati completamente dopo 180 giorni al termine contrattuale della convezione tra Ateneo, CRUI e Microsoft.

8. **Soggetti o categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Autorizzati**
   I dati trattati per le finalità di cui sopra verranno comunicati o saranno comunque accessibili ai dipendenti e collaboratori assegnati ai competenti uffici dell'Università degli Studi dell'Insubria, soggetti autorizzati dal titolare (art. 29 GDPR 2016/679).
   I dati relativi agli accessi (*log*) sono accessibili esclusivamente agli amministratori di sistema espressamente autorizzati dal Titolare e non saranno ulteriormente comunicati se non per adempiere specifici obblighi di legge o per identificare responsabili di abusi e/o attività illecite operate dall'interessato o da terzi a danno dell'interessato.
   La gestione e la conservazione dei dati personali raccolti avviene presso l'Università e/o presso fornitori di servizi necessari alla gestione tecnico-amministrativa che, ai soli fini della prestazione

richiesta, potrebbero venire a conoscenza dei dati personali degli interessati nominati quali Responsabili del trattamento a norma dell'art. 28 del GDPR.
L'elenco completo ed aggiornato dei Responsabili del trattamento è conoscibile a mera richiesta presso la sede del titolare.

9. Trasferimento dati all'estero

I dati sono generalmente conservati su territorio europeo ma per particolari motivazioni tecniche e di sicurezza è prevista la possibilità di trasferimento verso gli Stati Uniti con appositi addendum contrattualmente definiti.

9. Diritti dell'Interessato

Questi sono i diritti esercitabili nei confronti dell'Università degli Studi dell'Insubria (Titolare del trattamento):

- diritto di accesso ai propri dati personali ed a tutte le informazioni di cui all'art.15 del GDPR,
- diritto di rettifica dei propri dati personali inesatti e l'integrazione di quelli incompleti,
- diritto di cancellazione dei propri dati, fatta eccezione per quelli contenuti in atti che devono essere obbligatoriamente conservati dall'Università e salvo che sussista un motivo legittimo prevalente per procedere al trattamento;
- diritto alla limitazione del trattamento ove ricorra una delle ipotesi di cui all'art. 18 del GDPR.
- diritto di opporsi al trattamento dei propri dati personali, fermo quanto previsto con riguardo alla necessità ed obbligatorietà del trattamento ai fini dell'instaurazione del rapporto
- diritto di revocare il consenso eventualmente prestato per i trattamenti non obbligatori dei dati, senza con ciò pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca.

Per l'esercizio di questi diritti l'Interessato può rivolgersi al Responsabile della protezione dei dati inviando la richiesta via mail all'indirizzo privacy@uninsubria.it.

10. Reclamo

L'Interessato ha inoltre diritto di avanzare un reclamo al Garante per la Protezione dei Dati Personali (www.garanteprivacy.it) o all'Autorità Garante dello Stato dell'UE in cui l'Interessato risiede abitualmente o lavora, oppure del luogo ove si è verificata la presunta violazione, in relazione a un trattamento che consideri non conforme.