insights®

Insights Discovery for Microsoft Teams

Data Protection, Privacy and Security Guide

Setup

Item	Details
Document Name	Insights Discovery for Microsoft Teams- Data Protection, Privacy and Security Guide
Owner	Product Team
Version	1.0
Last Updated	5th June 2026
Audience	Data Protection Officers, Legal Teams, Security Teams
Purpose	Data Protection, privacy and security information

Version	Date	Description of Changes
1.0	5th June 2026	First published version

Setup

Table of Contents

What you need to know

Insights Discovery for Microsoft Teams brings existing profiles directly into Microsoft Teams, helping your people connect and collaborate more effectively. This guide details the essential security and privacy information you need to feel confident about deploying our app in your organisation. This integration brings the power of Insights Discovery directly into your daily Microsoft Teams experience, with robust security measures, transparent data practices, and comprehensive support. We've designed it to give IT teams confidence while helping your people work better together.

Who we are & our credentials

We're The Insights Group Limited and affiliates, headquartered in Scotland and registered with the UK Information Commissioner's Office. Here's some key information for your security assessment:

- **ISO 27001:2022 certified** (achieved November 2023)
- **Independent data controller** - we make our own data decisions, see our privacy notice
- **Full GDPR compliance** (UK GDPR, EU GDPR, Data Protection Act 2018)
- **Professional security testing** - independently assessed by Barrier Networks (June 2024)

Security testing

Our app underwent comprehensive professional security testing in 2024, including traffic analysis, dynamic testing, static code analysis, and SSL/TLS testing.

The results? Only 3 minor vulnerabilities were found (1 medium, 2 low risk) and **all have been fixed**. The retest confirmed no outstanding security issues.

The data we use

Only individuals who already have an Insights Discovery profile can use the app. However, to make the app work, it accesses certain basic Microsoft 365 directory data for every user in your organisation's directory - not only those with an Insights Discovery profile . When the app is used, we process the following :

- **Profile data** - your existing Insights Discovery profiles and colour preferences
- **Basic Microsoft info** - email, display name, profile photo, user ID

- **App settings** - language preferences and user customisation
- **Optional feedback** - collected 6 weeks after setup via our support bot

Directory data for all users (including those without an Insights profile)

Through two Microsoft Teams permissions, the app reads basic directory data for all users in your organisation, including those who do not have an Insights Discovery profile:

(a) Display name, first and last name, email address and profile photo for all users in the directory (User.ReadBasic.All); and

b) Presence, availability, status notes, out-of-office messages, timezone and location for all users in the directory (Presence.Read.All).

Where an individual does not have an Insights Discovery profile, the app processes their basic data only transiently (approximately 15 minutes) and solely to check whether a profile association exists and to display accurate status within the app. No Insights profile content is shown for those individuals because they do not have a profile.

What we don't collect: special category data

How we keep data safe

Secure hosting - AWS ISO 27001 certified data centres (UK and EU)
Smart caching - 24-hour refresh cycle for quick access
Encryption - applied wherever possible
Regular testing - annual penetration testing by certified specialists
Monitoring - continuous data integrity checks
Clean-up - secure disposal and 180-day security log retention

Microsoft Teams integration

Our app is built specifically for Microsoft Teams and requires certain permissions to work properly:

- **Application permissions** - needed for automatic bot installation and tab management
- **User permissions** (delegated, operating tenant-wide on behalf of the signed-in profile holder): User.ReadBasic.All - reads display name, first/last name, email address and profile photo for all directory users; and Presence.Read.All - reads activity, availability, status notes, out-of-office messages, timezone and location for all directory users. Also used for authentication and presence information within Microsoft Teams.
- **AppCatalog.Read.All** – Read all app catalogs (to locate the app's ID so it can be installed to meeting chats).
- **Calendars.Read** – Read user calendars (to show upcoming Teams meetings and the average Colour Energy of attendees).
- **ChannelMember.Read.All** – Read channel members (to display relevant Insights profile and communication tips).
- **Chat.ReadBasic** – Read names and members of chat threads (to display profile information for chat members).
- **People.Read** – Read the user's relevant people list (to retrieve people in meeting rooms).
- **Presence.Read.All** – Read presence of all users (to show availability, e.g. online/away, in the app tab).
- **TeamsAppInstallation.ReadWriteSelfForChat** – Allow the app to manage itself in chats (to add the Insights tab to a meeting chat).
- **TeamsTab.Read.All** – Read tabs in Teams (to check whether an Insights tab already exists and link to it).
- **TeamsTab.ReadWriteForChat** – Manage all tabs in chats (to add the Insights tab to a chat).
- **User.ReadBasic.All** – Read all users' basic profiles (to show profile images and link users to their Insights profile).
- **User.ReadWrite** – Read and write the user's profile (to let the user update their profile photo via the Avatar

tab).
- **User.Read** – Allow users to sign in and read their own profile.
- **openid** – Allow users to sign in.
- **profile** – Read users' basic profile details.
- **email** – Read users' primary email address.
- **offline_access** – Maintain access to data the user has granted.
- **TeamsActivity.Send** – Send activity notifications to users.

Why do we need these? to automatically install tabs in chats/meetings and show online status, providing the integrated Insights Discovery service within Microsoft Teams.
The app is a React web application that communicates securely with our platform via API. Updates happen automatically for security fixes, with Microsoft store approval needed for major feature changes.

Legal basis & EU compliance
For individuals with an Insights Discovery profile, the legal basis on which we process profile data is legitimate interests for providing learning and development services. For individuals who do not have an Insights Discovery profile, whose basic directory data is accessed transiently when a profile holder uses the app, our legal basis is also legitimate interests - specifically the operational need to check whether a profile association exists and to display accurate status within the app. We have completed a legitimate interests assessment confirming that this processing is necessary, proportionate and does not override the rights and freedoms of those individuals. We fully comply with data subject rights - erasure request result in immediate profile data removal (note: cached data in Microsoft Teams refreshes within 24 hours). We consider this to be low-risk processing that supplements our existing Insights Discovery product. If you need to undertake a DPIA for app implementation, we're happy to support with any information you need.
As controller, Insights facilitates data subject rights (access, rectification, erasure, restriction, portability and objection). Individuals - including those without an Insights profile - can exercise their rights or raise queries by contacting dpo@insights.com, and we will respond within one calendar month. If an employee raises a request with the customer directly in relation to the app, they should be directed to us.

Control, user privacy & data sharing

We take privacy seriously and have the following embedded in our offering:

Admin control - you decide who gets access through Microsoft Teams policies
User choice - individuals can make their profiles private or customise what is shared from their profiles
Tenant validation - we verify your organisation is set up before allowing access
Clear boundaries - only existing Insights customers with an Insights Discovery profile can use the app to view profile content.

The visibility of colour preferences and profile statements within Microsoft Teams can be completely turned off, if an individual chooses to do so. Equally, they can share all the information or select their preferences within the privacy settings of the app so that only specific statements can be viewed by colleagues. Where an individual communicates with another person from a separate organisation who also uses Microsoft Teams and the Insights Discovery app, neither party will be able to see profile data. Only those with the same Tenant ID organisation, can view this information when shared.
We share necessary data with Microsoft Corporation and its affiliates to make the app work, and with carefully selected suppliers providing IT, database and system administration services, including Amazon Web Services (AWS) as our cloud infrastructure provider. We never sell data to third parties. For transfers of personal data outside the EEA we rely on the EU Standard Contractual Clauses; for transfers originating from the United Kingdom we rely on the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, as applicable.
Because the app accesses basic directory data for everyone in your organisation, we recommend that you highlight Insights' Privacy Notice (available at www.insights.com/general-privacy-notice/) to all employees - including those who

do not hold an Insights Discovery profile - as part of your internal rollout communications, so that all individuals are appropriately informed before deployment.

Support & contact

Need help or have questions? Contact us here:
Technical setup: msteams@insights.com
Data protection: dpo@insights.com
Security: security@insights.com