Data Security & Privacy Policy

Microsoft 365 License Assessment

At NUDGEIT, we understand that granting access to your Microsoft 365 tenant requires trust. This document explains exactly how we handle your data during the License Assessment — what we collect, how we protect it, and when we delete it.

1. What We Access

Our assessment uses read-only permissions through Microsoft's standard OAuth consent flow. The entire process operates within the Microsoft ecosystem — no third-party services are involved in data collection or processing. We cannot modify, delete, or send any data in your environment. The registration link is tenant-specific, preventing cross-tenant access. The permissions we request are limited to:

Permission	Purpose
User.Read.All	Identify license holders and user profiles
Group.Read.All	Understand group memberships for user segmentation
Directory.Read.All	Read directory structure and organizational context
Organization.Read.All	Read tenant and organization details
Reports.Read.All	Access M365 usage reports to identify underutilization
AuditLog.Read.All	Analyze activity patterns over 180 days
MailboxSettings.Read	Read mailbox configuration settings
CallRecords.Read.All	Assess Teams usage for license optimization

We do not access: email content, file contents, OneDrive documents, SharePoint data, or chat messages. Only metadata and usage statistics are collected. Note: Due to Microsoft Graph API design, API responses may include additional metadata fields beyond what is strictly needed for the report — such data is not used in our analysis and is discarded. For PSTN call records, actual phone numbers are masked by Microsoft; we only see user identity and call duration.

2. Data Minimization

We follow a strict principle of data minimization:

- We collect only the data required to produce the assessment report.
- No unnecessary personal information is gathered or stored.
- User data is aggregated and anonymized in the final report wherever possible.
- Personal data collected includes names, email addresses, and department information — used only for license-to-user mapping and user segmentation. No telephone numbers or private addresses are collected. This data is not shared externally.
- Due to Graph API limitations, complete data sets are returned per API call. Only fields relevant to the assessment are processed; all other data is discarded and not retained.

3. Data Storage & Protection

Aspect	Details
Encryption in transit	All data transfers use TLS 1.2+ encryption
Encryption at rest	Stored data is encrypted using AES-256 (BitLocker on dedicated analysis machines, Azure Disk Encryption if processed on Azure VMs)
Data residency	Data is processed on a dedicated, certificate-secured NUDGEIT machine within our controlled environment. No data is transferred to third-party services.
Access control	Restricted to authorized NUDGEIT assessment personnel. The analysis application requires a machine-specific certificate to operate — only certified machines can execute the assessment.

4. Data Retention & Deletion

We retain assessment data only as long as necessary. Two scenarios apply:

- Assessment-only engagement: All collected tenant data is deleted within 14 days of delivering the assessment report.
- Ongoing optimization engagement: If you engage NUDGEIT for follow-up license changes, data is retained during the active optimization phase (for rollback/failback purposes) and deleted upon completion of the engagement.
- The final assessment report (anonymized) may be retained for reference if you engage NUDGEIT for follow-up services — otherwise it is also deleted.
- You may request immediate deletion of all data at any time by contacting info@nudgeit.com.

5. Access Is Temporary & Revocable

The consent you grant is for the purpose of this assessment only. A Global Administrator is required to grant the initial consent; ongoing operation does not require Global Admin privileges.

- Data collection requires only a single consent — no recurring authorization is needed. We do not maintain persistent access to your tenant beyond the assessment scope.
- You can revoke access at any time through two options: (1) Delete the Enterprise Application entirely from your Entra ID tenant (Entra Portal → Enterprise Applications → locate and delete the app), or (2) Disable sign-in for the service principal to block data access while keeping the registration.
- You can monitor all access to your tenant via Entra ID sign-in logs (Service principal sign-ins). These logs show exactly when our application accessed your data, and you can configure alerts for this activity.

6. Personnel & Confidentiality

Your data is handled with care:

- Only authorized NUDGEIT assessment specialists have access to your tenant data.

- All personnel involved are bound by confidentiality agreements.
- Data is never shared with third parties, including our distribution partners. The entire assessment process operates within the Microsoft ecosystem — no external tools or services are involved in data processing.

7. Your Rights

As a customer, you have the right to:

- Know exactly what data we collect (as described in this document).
- Request a copy of all data held about your organization.
- Request immediate deletion of your data at any point.
- Revoke tenant access at any time without prior notice.

8. Customer Prerequisites

To ensure a smooth and accurate assessment, the following prerequisites apply:

- A Global Administrator must grant the initial consent for the NUDGEIT assessment application.
- The “Show user details in reports” setting must be enabled in the Microsoft 365 admin center. If your organization has anonymized/obfuscated reporting enabled, this setting must be temporarily adjusted by your administrator for the duration of data collection.
- No additional software installation is required on your end — the assessment is performed entirely through Microsoft’s Graph API.

9. Audit & Transparency

We believe in full transparency regarding data access:

- All service principal sign-ins are visible in your Entra ID sign-in logs, providing a complete audit trail of when our application accessed your tenant.
- You can configure automated alerts in Entra ID to be notified whenever our service principal signs in.
- The assessment report can be regenerated at any time while the application remains registered in your tenant, giving you full control over the process.

Questions about data security?

Contact us at info@nudgeit.com — we’re happy to discuss any concerns before you proceed.