EMBEDDED SHADOW AI SCAN

The shadow AI you approved yourself

Prepared for Nordveld Instruments

Prepared by Prometheon · 16 June 2026 · Scope: 3 of 34 tools

Illustrative sample. Nordveld Instruments is a fictional 180-person European manufacturer used to show what a scan looks like. The three tool findings are **real and sourced** as of 16 June 2026 — every claim carries a numbered citation; full clickable references are on the last page. This is an indicative advisory read, not a compliance determination or audit.

What we did

You shared 34 tools your organization uses. We scanned **3** of them for embedded AI: the generative-AI features your vendors may have switched on inside software you already approved. For each tool we identified the vendor, reviewed their public product pages, release notes, privacy policy, and sub-processor disclosures, and translated that into what it likely means for your data exposure and your EU AI Act deployer duties.

Read this as a starting point, not a verdict. Every claim below carries a numbered citation [n] you can click to open the source; the full reference list is on the last page. Public documentation lags reality, so confirm specifics with each vendor before acting. Where the public sources do not establish something, we say “unclear from public sources” rather than guess. Low-confidence findings are capped at Amber.

Headline

3 / 34
tools scanned

3
have AI features

2
on/available with no explicit decision

RED 1 AMBER 2 · GREEN 0

Look at first: Microsoft SharePoint / Microsoft 365. Copilot reaches everything a user can already open across SharePoint, email and Teams [1], a free Copilot Chat tier is broadly available without a purchase decision [1], and over-sharing actively surfaces it [1]. The exposure is over-sharing plus governance, not Microsoft moving EU data out of the EU.

Findings

1. Microsoft SharePoint / Microsoft 365 (Copilot, Copilot Chat, SharePoint agents)

RED confidence: high

AI feature	Microsoft 365 Copilot (grounded in your data via Microsoft Graph) [1], the free Microsoft 365 Copilot Chat [8], and SharePoint agents [7].
On by default?	Partly. Full Copilot needs a paid licence [7], but Copilot Chat is free and broadly available [8]. The Copilot app also auto-installs on managed Windows (EEA excluded, so NL is spared) and was temporarily paused in May 2026 [4].
Data it can reach	Everything the individual user can already open: SharePoint sites and files, OneDrive, Exchange mail and calendar, Teams chats. It respects permissions [1], but surfaces content that was over-shared and never meant to be found [5].
Where processed	Microsoft 365 service boundary (Azure OpenAI); EU Data Boundary for EU customers; not used to train foundation models [1,2]. In-country processing is rolling out [9]. Watch-item: Anthropic is a named sub-processor outside the EU Data Boundary, off by default for EU/EFTA/UK, verify [3]. Provider is US-parented (CLOUD Act not addressed in the docs).
Deployer flag	EU AI Act Art. 26: you own human oversight of Copilot output, usage logging (Microsoft Purview can satisfy this), and informing staff before workplace use [19].
Why Red	It reaches your most sensitive content at scale, over-sharing actively surfaces it, the free Chat tier needs no purchase decision, and the provider is US-parented. Restricted SharePoint Search and Restricted Content Discovery are **not** security boundaries, do not treat them as the fix [5,6].
Verify	Who actually holds Copilot licences; governance of free Copilot Chat; run SharePoint Advanced Management data-access-governance reports and apply sensitivity labels / Restricted Access Control before Copilot spreads [6,7]. Confirm Anthropic is off in your tenant region [3], and turn on Purview audit.

2. Exact Online (Exact AI Assistant + AI agents)

AMBER confidence: medium

AI feature	Exact AI Assistant, a generative assistant launched 20 Nov 2024 [11], plus ML "agents" (Purchase, Bank, Debtor and more) that auto-process invoices and match transactions [10].
On by default?	No. It is user-invoked and does not appear on screen by default [11]. Users can enable or disable it [10]. Whether it is admin-gated or needs a paid module is unclear from public sources.
Data it can reach	Financial records, invoices, GL postings, debtor and customer data, 40+ KPIs [10]. Underlying records routinely hold personal data and, in HR/payroll, BSN and salary data [13].
Where processed	Platform hosting in the EEA (Azure and AWS in the EEA; hosting also in the Netherlands) [13]. The AI inference provider/model is **not publicly named** and the only public sub-processor list (2022) predates the AI Assistant [13]. "Never used to train **general** AI models" (note the hedge) [10].
Deployer flag	EU AI Act Art. 26: human oversight of financial automation; worker notification where AI touches HR/payroll data [19].
Why Amber	Not on by default and EEA platform hosting pull it below Red, but it touches sensitive financial and personal data while the AI provider and AI-layer residency are undisclosed. Medium confidence, so capped at Amber.
Verify	Request Exact's **current** AI sub-processor annex and the model/provider behind the Assistant; confirm AI prompts stay in the EEA at the inference layer; pin down the "no training" scope contractually (does it also exclude Exact's own models?) [13].

3. AFAS (the "Jonas" AI assistant)

AMBER confidence: medium-high

AI feature	“Jonas”: AI-composed workflow replies, summarization, translation, voice-to-text (incl. performance reviews), receipt/CV recognition and candidate-to-vacancy matching [14,16].
On by default?	Mostly admin-activated / opt-in (“AI where we use third parties is always based on activations”) [15]. Exception: receipt recognition in AFAS Pocket is on by default [16].
Data it can reach	HR and personnel records, recruitment data (CVs, candidate matching), performance-review content, financial and receipt data, much of it special-category personal data [14,16].
Where processed	In the EEA. Core hosting at Leaseweb data centres in the Netherlands, not AFAS’s own [18]. Generative features run on Azure OpenAI within the EEA and AFAS’s own tenant; speech-to-text uses in-house models; not used to train; AFAS has a Chief AI Compliance Officer and states it works “in line with the EU AI Act” [15,17].
Deployer flag	EU AI Act Art. 26, heightened: HR and recruitment AI can be higher-risk; run a DPIA and inform affected workers [19].
Why Amber	Strong EEA/NL hosting, mostly opt-in and no-training pull toward Green, but it touches sensitive HR data, has a default-on feature, and recruitment AI is higher-risk under the AI Act.
Verify	Disable Jonas features you do not need (especially Pocket receipt recognition); run a DPIA on recruitment and review-transcription AI; request the current sub-processor register and reconcile the “Azure Foundry own tenant” vs “Azure OpenAI” wording [15].

What this suggests for you

- **Review first (Red):** Microsoft 365 / SharePoint. Fix the over-sharing posture and govern the free Copilot Chat tier before Copilot spreads further.
- **Govern and assign an owner (Amber):** Exact Online and AFAS. Get the AI sub-processor answers in writing, disable features you do not use, and run a DPIA where HR data is involved.
- **The deployer gap:** under the EU AI Act you own oversight, logging and (for workplace tools) worker notification for all of the above, including features you did not switch on [19]. The durable fix is a small process so the **next** silent rollout reaches a named owner.
- **Sovereign-migration signal:** your most sensitive content (SharePoint IP, payroll data) is reachable by AI running on US-parented infrastructure [1,3]. That is the trigger to decide, workload by workload, what should move onto sovereign infrastructure.

The other 31 tools

This scan covered 3 of your 34 tools. The full **Embedded Shadow AI Assessment** covers your whole stack, flags your EU AI Act deployer exposure per tool, gives your board a one-page decision sheet, and folds into an **EU AI Act + NIS2 readiness roadmap** (the EU AI Act applies directly in every member state; NIS2 applies through your country's own transposing law). Where regulated data is reaching foreign-controlled AI, that is the trigger for a **Sovereign Migration Assessment**, and for the highest-value workflows, for moving them onto **Theon**, our sovereign on-premise AI platform, where your data never leaves your environment.

This is advisory readiness, **not a certification audit**. We map your gaps and prepare you for official supervision under the EU AI Act and NIS2 by your national competent authorities. When you need a formal audit or legal sign-off, we hand off to an accredited partner.

IN DEVELOPMENT · EARLY ACCESS

Embedded AI Watch — never be the last to know

A scan is a snapshot; your vendors ship changes every week. We are building a continuous-monitoring subscription that keeps the software inventory from this scan **live**, and watches each of your vendors for the signals that matter: a new AI feature, a feature switched on by default, a new AI sub-processor, or a change in where your data is processed. It is the "small process so the next silent rollout reaches a named owner" that the deployer-gap finding above calls for, run for you.

The moment we detect one, ideally the day the vendor announces it, you get a **decision card**: what changed, what data it touches, the EU AI Act deployer implication, and a recommended **classify / approve / monitor / restrict** action, ready for your change-approval process. You decide up front, instead of finding out after it shipped. Delivered as a live watchlist dashboard with a weekly digest and instant high-impact alerts to email, Slack or Teams.

Want early access? Ask us when we run your full software list.

Want us to run your full software list?

Book a free 30-minute readiness intake and we will scope it with you.

Book your Embedded Shadow AI Scan readiness intake

References

All findings reflect public vendor documentation as of 16 June 2026, which can change without notice. Click any citation number in the report, or any link below, to open the source.

Microsoft 365 / SharePoint

[1] Microsoft Learn — Microsoft 365 Copilot: data, privacy, and security
https://learn.microsoft.com/en-us/microsoft-365/copilot/microsoft-365-copilot-privacy

[2] Microsoft Learn — Enterprise data protection in Microsoft 365 Copilot
https://learn.microsoft.com/en-us/microsoft-365/copilot/enterprise-data-protection

[3] Microsoft Learn — Connect to an AI subprocessor (Anthropic)
https://learn.microsoft.com/en-us/microsoft-365/copilot/connect-to-ai-subprocessor

[4] Microsoft Learn — Deploy the Microsoft 365 Copilot app (auto-install behaviour)
https://learn.microsoft.com/en-us/microsoft-365/copilot/deploy-microsoft-365-copilot-app

[5] Microsoft Learn — Restricted SharePoint Search (oversharing worked example)
https://learn.microsoft.com/en-us/sharepoint/restricted-sharepoint-search

[6] Microsoft Learn — Restricted Content Discovery
https://learn.microsoft.com/en-us/sharepoint/restricted-content-discovery

[7] Microsoft Learn — Manage access to agents in SharePoint
https://learn.microsoft.com/en-us/sharepoint/manage-access-agents-in-sharepoint

[8] Microsoft 365 blog — Introducing Microsoft 365 Copilot Chat (free tier), 15 Jan 2025
https://www.microsoft.com/en-us/microsoft-365/blog/2025/01/15/copilot-for-all-introducing-microsoft-365-copilot-chat/

[9] Microsoft 365 blog — In-country data processing for Copilot, 4 Nov 2025
https://www.microsoft.com/en-us/microsoft-365/blog/2025/11/04/microsoft-offers-in-country-data-processing-to-15-countries-to-strengthen-sovereign-controls-for-microsoft-365-copilot/

Exact Online

[10] Exact — Artificial intelligence
https://www.exact.com/us/about-us/artificial-intelligence

[11] Exact — 'A PA for everyone': Exact AI Assistant launch (20 Nov 2024)
https://www.exact.com/news/a-pa-for-everyone-that-is-the-idea-behind-exact-assistant

[12] Exact — Trust & certifications
https://www.exact.com/trust/certifications

[13] Exact — Data processing agreement / sub-processors (2022)
https://files.exact.com/static/downloads/information-security/E-MKB-BIJLAGE-VERWERKERSOVEREENKOMST-202207.pdf

AFAS

[14] AFAS — Software & AI
https://www.afas.nl/software/ai

[15] AFAS — How we handle AI (themapagina)
https://www.afas.nl/portal-themapagina/afas-ai-hoe-gaan-we-bij-afas-om-met-ai-afas-software

[16] AFAS — Jonas help centre
https://help.afas.nl/help/NL/SE/jonas.htm

[17] AFAS — Data sovereignty
https://www.afas.nl/continuiteit/data-soevereiniteit

[18] AFAS — AFAS Online architecture (hosting)
https://klant.afas.nl/afas-online/architectuur

EU AI Act

[19] EU AI Act — Article 26: obligations of deployers of high-risk AI systems
https://artificialintelligenceact.eu/article/26/