PC | SCHEMATIC®

AI Assistant

Privacy, Hosting and Security

For

PC | Automation™

Version 1.2 · August 2026 · PC SCHEMATIC A/S

Contents

Contents 2
About this document 3
Executive summary 3
1. What the AI Assistant is 3
2. How it works 4
2.1 The data flow in detail 4
2.2 Who processes your data 5
3. Your data stays yours 5
4. You stay in control 5
5. Where it runs 5
6. Built and operated securely 6
7. Compliance and standards 6

About this document

This white paper is for the security officers, data-protection officers, and IT decision-makers who are evaluating or rolling out the PC SCHEMATIC | AI Assistant. It explains, at a high level, how the product handles your data, where it runs, and the guarantees we make.

It is deliberately concept-level: it describes how we operate and what we commit to, not the internal mechanics. PC SCHEMATIC A/S continuously improves the product, so implementation details may evolve.

Executive summary

The AI Assistant puts an AI engineering copilot next to your electrical CAD project without asking you to give up control of your data. Three principles run through the whole product:

> **1. Your data stays yours.** Secrets and personal data are removed before anything leaves your workstation, and no model provider trains on your content.
>
> **2. European, isolated hosting.** The service runs in the EU, your data is kept isolated from other customers, the AI model is never exposed to the public internet and is fully sandboxed.
>
> **3. You stay in control.** The assistant proposes changes; you approve them. Key actions are recorded for audit.

The product is designed and operated to align with the EU General Data Protection Regulation (GDPR), the NIS2 Directive, the EU AI Act, and the EU Cyber Resilience Act.

1. What the AI Assistant is

The AI Assistant is an AI copilot in a chat panel beside PC SCHEMATIC | Automation, your electrical CAD application. You ask for what you want in plain language; it inspects the currently open project, attached files, and files in the user folder, and answers the question or command you gave it.

It will answer anything related to electrical concepts, components, and your project (e.g. “what is a contactor used for?” or “Check my project for short circuits.”), but will not answer unrelated questions (e.g. “What will the weather be like tomorrow?”).

Answers may be a text reply, or it may (with approval) take certain actions:

- Navigate the project
- Build and export lists to excel and CSV files
- Correct spelling in project
- Search the web

The AI Assistant CANNOT make edits to your project or look at several open projects.

Part of it runs on your own machine, and a secure cloud service connects it to an AI model. It is a focused engineering assistant, not a general-purpose chatbot: it works only on the project you have open and politely declines off-topic requests.

2. How it works

Your workstation talks to the PC SCHEMATIC cloud service over an encrypted connection. The service signs you in, removes sensitive data, and forwards only safe, tokenized text to an EU-hosted AI model. The answer returns the same way, and your real values are restored only on your own device.

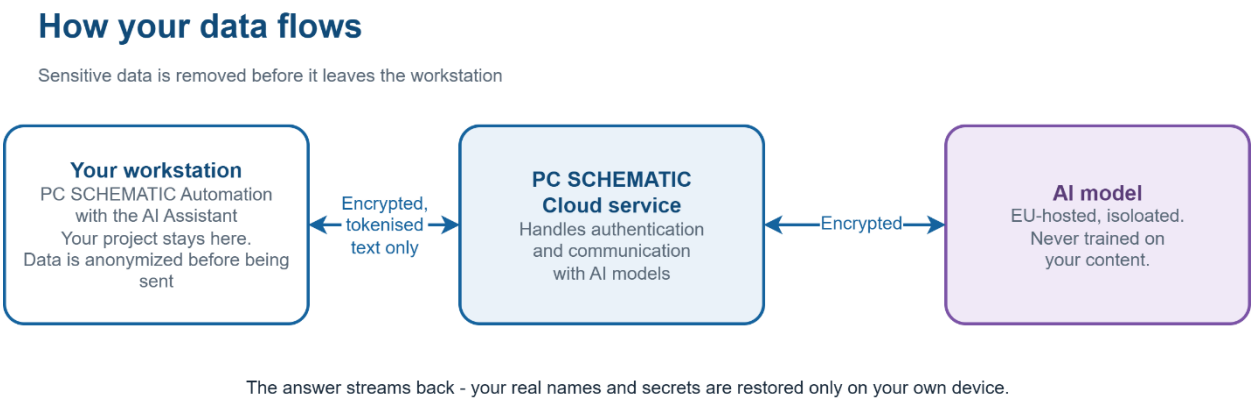


Figure 1. How your data flows. Sensitive data is removed on your workstation, before it hits the cloud service, and before anything reaches the AI model; real values are restored only on your device.

The AI model operates under a contract that prevents it from training on your content. Because sensitive data is removed before anything is sent, the model only ever works with a placeholder context, never your real secrets or personal data.

2.1 The data flow in detail

- **On your device.** The chat window, the AI agent, and the integration with PC SCHEMATIC | Automation all run locally on your machine. Project data is read locally, and only the content relevant to the specific request leaves the device. Your chat history is stored exclusively on your own machine.
- **Filtering before anything is sent.** Before a request leaves your device, built-in filtering removes known secrets (API keys, passwords, connection strings) irreversibly, and replaces personal data such as e-mail addresses, national ID numbers, IBANs, and phone numbers with pseudonyms. The key needed to translate the pseudonyms back exists only in memory on your own device and never leaves it.
- **PC SCHEMATIC's gateway in the EU.** The request is sent TLS-encrypted to our gateway, which is operated by PC SCHEMATIC A/S and runs in Microsoft Azure in the EU (Sweden Central, with supporting services in West Europe). The gateway validates your organization's API key and forwards the request. It does not store the content of your messages — only consumption data for billing (timestamp, model, token count, and a pseudonymized installation ID), which is kept for 12 months.
- **The AI model.** The gateway calls an Azure OpenAI model in Microsoft Azure — either a dedicated deployment created specifically for your organization (reachable only over a private network, with no public access), or our shared EU deployment. Model inference itself is locked

to the EU data zone (Azure “Data Zone Standard”), and requests are processed without server-side storage of conversations at Microsoft.

2.2 Who processes your data

- PC SCHEMATIC A/S operates the gateway and acts as data processor.
- Microsoft (Azure OpenAI) hosts the gateway and runs the AI model itself, as sub-processor. Microsoft is contractually committed not to train models on your data, not to share it with OpenAI (the company), and not to make it available to other customers.
- OpenAI (the company) never receives your data. The model runs exclusively in Microsoft's European data centers, and nothing is sent to OpenAI's own systems.

3. Your data stays yours

This is the most important promise in the product: **sensitive data never leaves your workstation and therefore never reaches an AI provider.** Before any request leaves your workstation, the AI Assistant tokenizes your data, a feature that cannot be switched off.

4. You stay in control

Because the assistant can act inside your CAD project, you stay in charge of every change:

- It proposes changes; nothing is applied to your project unless you approve it.
- It can act only inside the project you have open, using a fixed, pre-approved set of actions.
- Key actions are recorded, so there is always an audit trail of what happened.

For managed fleets, the assistant's configuration can be locked so it cannot be quietly redirected to anything other than the approved service.

5. Where it runs

The cloud service runs on established European cloud infrastructure, hosted in the EU. The underlying platform is independently certified against recognized security standards such as ISO 27001 and SOC 2, and we add our own controls on top.

- All data is encrypted in transit and at rest.
- Access is governed by identity, with least-privilege permissions.
- The AI model is not reachable from the public internet.
- Isolation is per user, not just per organization. Even colleagues in the same company cannot reach each other's context, projects, messages, and everything else stay private to the user they belong to.
- The AI model runs in the Azure OpenAI EU data zone, with primary processing in Sweden Central and supporting services in West Europe.
- Customers who require it can be provisioned a dedicated, single-tenant model deployment, reachable only over a private network and never exposed to the public internet.

6. Built and operated securely

Security is built in from the first line of code, not bolted on afterwards.

- Every change is peer-reviewed and passes automated security checks before it ships.
- We track the third-party components in every release, so we can respond quickly when a new vulnerability is disclosed.
- We run regular internal security reviews against GDPR, NIS2, EU AI Act, and the EU Cyber Resilience Act; findings are remediated and re-verified.
- In production we monitor continuously, keep audit trails of key actions, and follow documented incident-response procedures.

7. Compliance and standards

The AI Assistant and its cloud service are designed and operated to align with the EU General Data Protection Regulation (GDPR), the NIS2 Directive, the EU AI Act, and the EU Cyber Resilience Act. Hosting is in the EU, and the processing of personal data is governed by our Data Processing Agreement.