



TOPdesk AI Policy

Version 2.0 – effective 01-04-2026

1. Purpose and Scope

This AI Policy outlines the purpose and use of AI-assisted service management within the TOPdesk SaaS and On-Premise Platforms. It defines the applicable roles under [Regulation \(EU\) 2024/1689](#), also known as the EU Artificial Intelligence Act (AI Act), for each AI system and describes TOPdesk’s approach to responsible artificial intelligence (AI) governance and acceptable use. Together, these measures ensure compliance with EU requirements on transparency and accountability in the use of artificial intelligence.

The AI Policy supplements the TOPdesk [Privacy Statement](#) and applies when customers use AI-assisted service management functionalities offered by TOPdesk.

2. AI System Inventory

In line with the AI Act, TOPdesk maintains an inventory of all AI systems that are, or could be, used within its Platform.

Within our AI-assisted service management, we need to distinguish three (3) types of AI systems:

- **AI Automations:** AI implementations that a TOPdesk consultant can configure between the customer’s SaaS environment and the Large Language Model (LLM) used by the customer.
- **AI Features:** AI implementations embedded within the TOPdesk SaaS software that use AI models made available via Microsoft Foundry (Azure).
- **Partner AI Solutions:** integrations with AI Solutions developed by third-parties.

AI Automations

TOPdesk consultants can implement AI Automations within the SaaS environment of the customer. These Automations use the customer’s own LLM. The customer is responsible for procuring, configuring and maintaining the LLM and assessing the risks involved in using this specific LLM. TOPdesk does not supply or operate the LLM and does not determine the purposes of processing data.

TOPdesk currently offers two (2) types of AI Automations that contain multiple different automations:

1. *Smart Incident Management with Generative AI*
2. *Smart Knowledge Item Management*

More information about the specific Automations is available through [my.TOPdesk](#). Please refer to 'Integrate and automate' and 'Set up AI-assisted automations'.

AI Features

TOPdesk introduces new AI Features that customers can implement within their SaaS environment. These Features are optional and disabled by default. An application manager of the customer must actively enable them (opt-in) within the secure operator section. Enabled AI Features can be disabled at any time.

TOPdesk currently offers the following AI Features:

1. *AI Incident categorization*
2. *AI Incident summarization*
3. *AI Knowledge item generation*
4. *AI Search*
5. *AI Writing assistant*

More information about the specific Features is available within the manuals page, that can be referenced through the secure operator section or through [my.TOPdesk](#).

The AI Features are hosted on Microsoft Azure and use one or more AI models made available via [Microsoft Foundry Catalog](#). The underlying AI models can include LLMs and other foundation models (e.g. text-classification models) offered directly by Microsoft or by selected third-party providers through the Microsoft Foundry Catalog.

The exact models and configurations used for each AI Feature may change over time as TOPdesk optimizes performance, quality, and compliance, without prior notice, provided that data protection and security standards remain at least equivalent.

Partner AI Solutions

TOPdesk offers integrations with third-party AI Solutions, such as the Ebbot chatbot and the TicketBuddy assistant. Details and availability of third-party AI Solutions are provided in my.TOPdesk and the TOPdesk Marketplace.

The use of these Solutions is governed exclusively by the applicable terms, conditions, and privacy notices of the respective third-party providers. By enabling a third-party Solution, the customer acknowledges and agrees to be bound by those terms.

TOPdesk does not control, operate, or manage third-party AI Solutions and is not responsible for their availability, performance, data processing practices, or the outcomes produced by such Solutions. Accordingly, third-party AI Solutions are outside the scope of this AI Policy and are not further addressed herein, as they are regulated exclusively by the third party's applicable agreements.

3. Legal Framework and Roles

All implementations described qualify as AI systems under the AI Act. The following role distinctions are aligned with the definitions provided in the AI Act to ensure that legal and operational responsibilities are clear.

AI Automations

Actor	Legal Role	Reasoning
Customer's LLM Provider	<i>Provider of the general-purpose AI model (GPAI)</i>	LLM Provider develops and hosts the general-purpose foundation model
TOPdesk	<i>Provider</i>	Since TOPdesk consultants tailor the AI Automation to the customer's use case, TOPdesk qualifies as a provider of the AI System
Customer	<i>Deployer</i>	Customer uses the AI system under its own authority and determines its purpose (e.g. HR, FM, IT)
End-user	<i>User</i>	End-user interacts with AI output (e.g. automated suggestions or summaries) but does not control deployment or compliance responsibilities

AI Features

Actor	Legal Role	Reasoning
Underlying model provider(s) accessed via Microsoft Foundry	<i>Provider of the general-purpose AI model (GPAI)</i>	The underlying model provider(s) develop and host the foundation models used by the AI Features
TOPdesk	<i>Provider</i>	TOPdesk integrates these GPAI models into its SaaS software, adds functionality, defines the system's intended purpose, and markets it under its own brand. This means that TOPdesk qualifies as the provider of the AI system
Customer	<i>Deployer</i>	Customer uses the AI system under its own authority and determines its purpose (e.g. HR, FM, IT)
End-user	<i>User</i>	End-user interacts with AI output (e.g. automated suggestions or summaries) but does not control deployment or compliance responsibilities

4. Risk Classification and Disclosures

Under the AI Act, the classification of an AI system as “high-risk” primarily depends on its intended purpose and deployment context. The AI Act’s risk-based framework distinguishes between prohibited AI practices, high-risk AI systems, and AI systems that are primarily subject to transparency obligations.

The **AI Features** and **AI Automations** offered by TOPdesk are designed to support service management workflows, such as drafting, suggesting, structuring, or preparing content, and do not autonomously make decisions that produce legal or similarly significant effects. Both are designed to ensure that humans remain in command at all times. When AI Features are enabled, end-users are clearly informed within the product when content or output is AI-generated or AI-assisted. In view of these safeguards and the intended purposes of the AI Features and AI Automations, they do not qualify as high-risk AI systems under the AI Act.

AI Features and AI Automations are not intended to be deployed in contexts that correspond to high-risk use cases listed in Annex III of the AI Act, such as automated decision-making in recruitment and selection, evaluation of performance at work, promotion or demotion decisions, or comparable decision-making contexts. However, if a customer deploys or configures AI Features or AI Automations for such purposes, the risk qualification of the overall system may change and could result in the system being classified as a high-risk AI system under the AI Act.

Where the customer deploys or configures TOPdesk AI Features or AI Automations in a context corresponding to a high-risk use case as listed in Annex III of the AI Act (including, without limitation, employment-related decisions such as recruitment, selection, performance evaluation, or promotion/demotion), the customer does so at its own risk and for its own account and is solely responsible for the resulting risk classification and all associated legal obligations. TOPdesk shall not be (and cannot be held) liable for any loss, damage, regulatory action, fines, or claims arising from such deployment or configuration by the customer.

Moreover, customers remain responsible for establishing appropriate internal governance and operational processes to ensure that end-users:

- review AI-generated or AI-assisted outputs and, where appropriate, override such outputs before taking final actions or making decisions;
- receive AI-literacy training appropriate to their roles and responsibilities; and
- understand how to identify and report anomalies, errors, or incidents to their application manager and/or TOPdesk.

5. Data Use, Privacy and Sensitive Data

Data processed in relation to **AI Automations** is governed by the data use, security and privacy terms of the selected LLM provider. Customers are responsible for reviewing and ensuring compliance with these provisions.

The General Data Protection Regulation (GDPR) applies whenever **AI Features** process personal data. Customers act as data controllers for their own use of the AI Features. TOPdesk acts as data processor and implements appropriate technical and organizational measures in line with the applicable Data Processing Agreement (‘DPA’) between customer and TOPdesk.

The AI Features process only the data necessary to perform the specific action requested by the user. This means that only the minimum data required to generate the requested output, such as the prompt, relevant context, and system parameters, are sent to the LLM. No additional or unrelated customer data are

transmitted. Inputs and completions are temporarily processed for inference and, where required, brief security or abuse monitoring. Depending on the specific AI Feature and Microsoft service capability used, certain data may also be stored temporarily where required for service functionality, security or abuse monitoring.

TOPdesk automatically removes personally identifiable information (PII) from defined action fields used by the AI Features. However, PII or special-category data contained within the free-text content body are not filtered and could be transmitted to the AI models used by TOPdesk via Microsoft Foundry when that content is used by an AI Feature. Customers must (i) avoid entering special-category data into free-text fields when using AI Features, or (ii) not use AI Features for content containing special-category data, or (iii) ensure a valid legal basis for the processing of special-category data exists which is based on the GDPR and provide appropriate information to end-users.

Data used with regard to the AI Features, such as prompts, completions, embeddings and training data, sent to Microsoft, are processed in line with Microsoft's data protection commitments for the relevant Microsoft Foundry service. In all cases, customer data are handled as follows:

- It is processed within Microsoft-managed Azure infrastructure and is logically isolated from other customers.
- TOPdesk does not permit AI Models to use prompts, completions, embeddings or training datasets to be used to train, retrain or otherwise improve any shared generative AI foundation models operated by Microsoft, the model provider, or any other third party, without the customer's explicit permission or instruction.
- TOPdesk does not share prompts or outputs with external model providers outside Microsoft Foundry.

More information about data privacy and data handling in Microsoft Azure Foundry is available on Microsoft's [website](#) and [Trust Center](#).

6. Incident Monitoring and Prohibited Practices

Both the Provider and the Deployer share responsibility for safe operation. Customers must promptly notify TOPdesk of any serious incident (malfunction, bias, or output error). TOPdesk maintains post-market monitoring procedures to investigate and remedy incidents in line with the AI Act.

To ensure the responsible and secure use of TOPdesk's AI features, customers must not use the **AI Features** for any prohibited practices as defined in the Microsoft [Code of Conduct](#). This includes, but is not limited to, using the Features to:

- Manipulate individuals or exploit their vulnerabilities.
- Generate unlawful, discriminatory, or misleading content.
- Deploy outputs for automated decision-making in designated high-risk domains (such as employment, education, healthcare, justice) unless applicable AI Act obligations are fulfilled.

Microsoft operates abuse monitoring and content-safety systems for models accessed via Microsoft Foundry. These systems use algorithms and heuristics to detect patterns of potentially abusive behaviour or content that may violate the applicable [Microsoft Code of Conduct](#) or Product Terms. If a violation is identified, the Customer will be notified. TOPdesk does not log or store the specific prompts or completions that triggered the violation beyond what is necessary for incident handling.

7. Data Retention

Data processed in relation to **AI Automations** is handled in accordance with the retention periods defined by the LLM used by the customer.

All **AI Features** process data in accordance with paragraph 5.

Data related to AI incident categorization is also stored. Data processed in connection with this Feature is retained only for as long as necessary to support the operation of the relevant AI Feature. After this period, the data is either deleted or anonymized.

8. Deployment Regions

Data processed in relation to **AI Automations** is handled in accordance with the specific restrictions defined by the LLM used by the Customer.

For **AI Features** provided by TOPdesk, data is sent to and processed within Microsoft Azure data centers using Microsoft Foundry models. Models within Microsoft Foundry offer different deployment types (e.g. Global, regional and DataZone deployments) that determine where inference data is processed and how data at rest is stored.

Processing of data for AI Features is restricted to specific regions. TOPdesk only uses AI models that support DataZone deployments within Europe (including the United Kingdom) and the United States. Under any deployment labelled DataZone, prompts and responses are processed within the designated data zone, and data stored at rest, such as uploaded content, is retained within the customer's specified geography.

- Data from customers within Europe is processed within Europe.
- Data from customers within the United States is processed within the United States.

For customers in other regions TOPdesk uses available deployment options. This means that prompts and responses may be processed in any geography where the selected AI model is available.

Regardless of the deployment type, data stored at rest remains within the designated Azure geography, while inference data is processed according to the selected deployment type. Furthermore, these AI services are subject to Microsoft's Data Protection Addendum and the applicable data protection terms for Azure. More information about deployment types and regions can be found on the Microsoft [website](#).

9. Changes to Policy and AI Systems

TOPdesk reserves the right to update or amend this AI Policy to reflect changes in legislation, technology, or internal practices. In the event of substantial changes to this Policy, customers will be informed in a timely manner through appropriate communication channels.

Substantial updates to AI systems will be announced in advance. Such updates will require renewed enablement by customers in the secure Operator Section before the updated AI systems can be used.

10. Contact

Questions about this AI Policy can be directed to: productupdate@topdesk.com