PUBLISHED: July 2026

Trusty Compliance Platform AI Integration & Usage

Overview

This document provides information on the usage of artificial intelligence (AI) within the Trusty Compliance Platform, detailing the AI models used, their application, and data handling practices.

AI Models Used in Trusty Compliance Platform

The platform utilizes the following AI models, powered by OpenAI technology and hosted by Azure AI on a European endpoint:

- **GPT-5 Mini** – A variant of GPT-5, balanced performance and cost for moderate reasoning tasks, also hosted by Azure AI on a European endpoint.
- **GPT-5 Nano** – A variant of GPT-5, Ultra-fast, low-latency model for high-throughput workloads, also hosted by Azure AI on a European endpoint.

Prior to **April 1st, 2025**, the platform used AI models hosted directly by OpenAI; since then, all AI processing has run on Azure AI-hosted models to ensure data residency within Europe.

Are These AI Models Open-Source?

No, these models are proprietary to OpenAI and not open-source.

How AI Processes Data

- Data is transmitted securely via API calls to Azure AI's infrastructure, which hosts OpenAI models on European endpoints.
- These endpoints are subject to strict European data protection regulations, including GDPR, ensuring that data privacy and sovereignty are maintained.
- AI processes input in real-time and returns responses based on the provided context.
- The Trusty Compliance Platform enforces strong encryption protocols to safeguard sensitive data during transmission.

Is Client Information Shared with Third Parties?

- Client data submitted to AI is processed exclusively by Azure AI on European endpoints and is not shared with any other AI provider.
- Azure AI does not retain API request data for training or any other purpose.
- Where screening features require external data sources (e.g., search engines and sanctions/PEP data providers), only the minimum data needed to perform the check (such as the name being screened) is transmitted to those processors, as detailed in our Data Processing Agreement.
- Each Trusty Compliance Platform account operates independently, ensuring complete data isolation with no cross-account access.
- Hosting on European Azure endpoints provides additional assurance through compliance with EU privacy standards and heightened sensitivity to the handling of personal data.

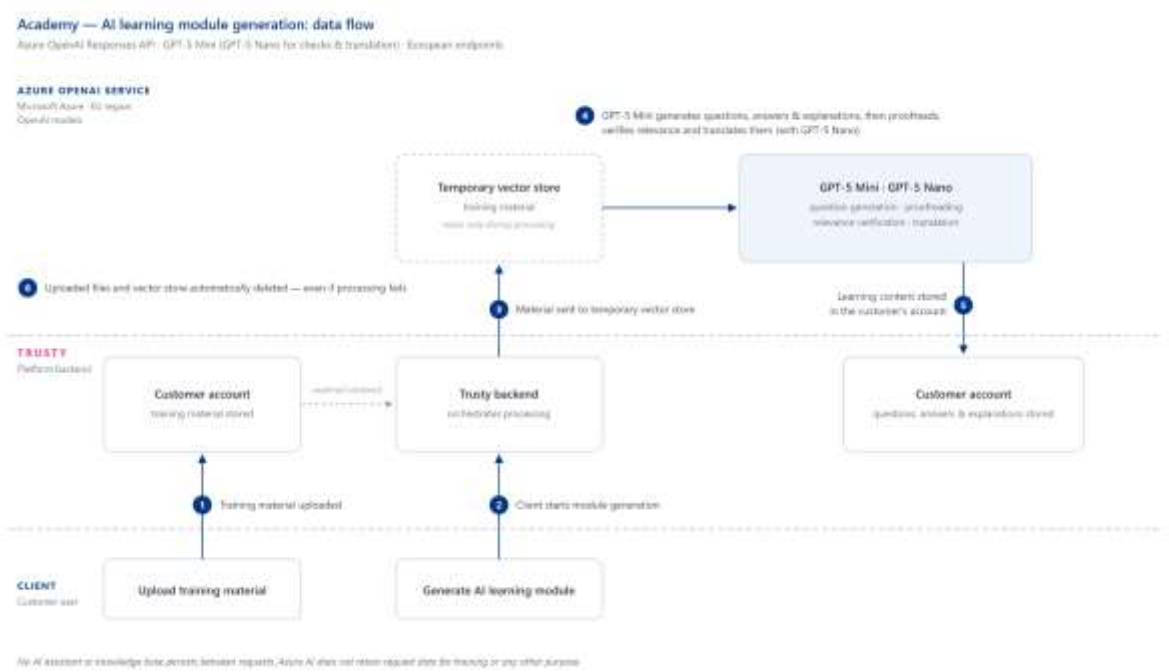
TRUSTY

AI Usage Across Trusty Compliance Platform Solutions

Trusty Whistleblowing Software

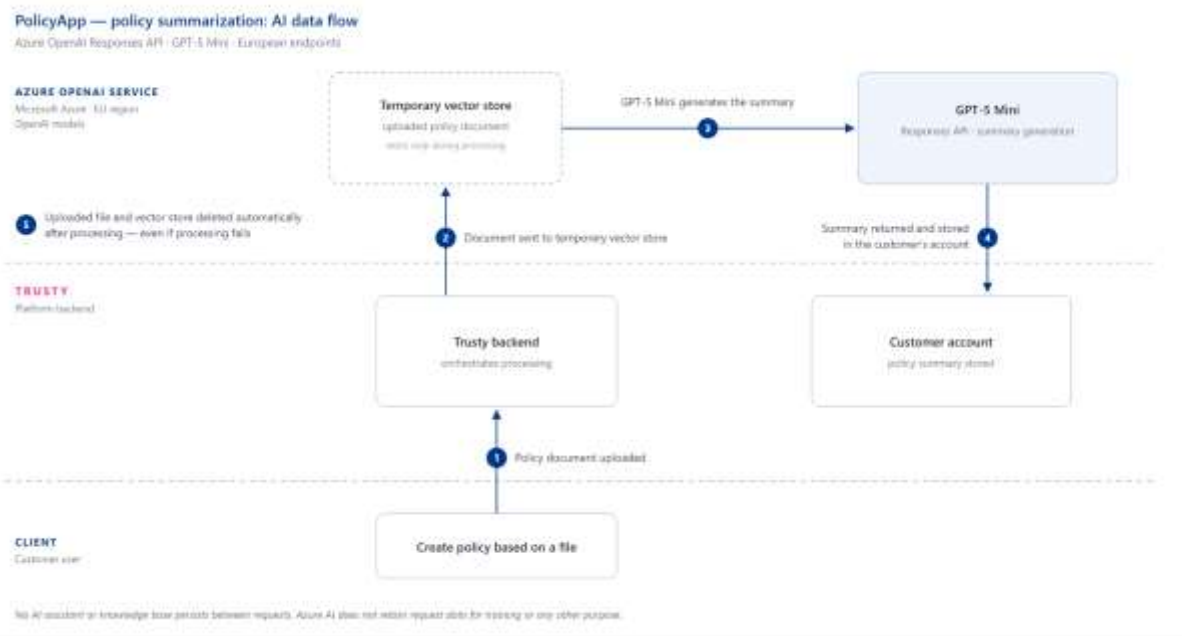
- AI Model: GPT-5 Mini
- Functionality:
    - Case summarization
    - Proposed additional questions for the whistleblower
    - Proposed actions
    - Case categorization
    - Chat

Academy



- AI Model: GPT-5 Mini (GPT-5 Nano for translations)
- Functionality:
    - AI generates training questions and answers.
    - It provides explanations for incorrect responses.
    - AI proofreading of generated questions/answers.
    - AI relevance/compliance-topic verification of generated questions.
    - AI translation of generated questions, answers, and explanations into the training's languages.

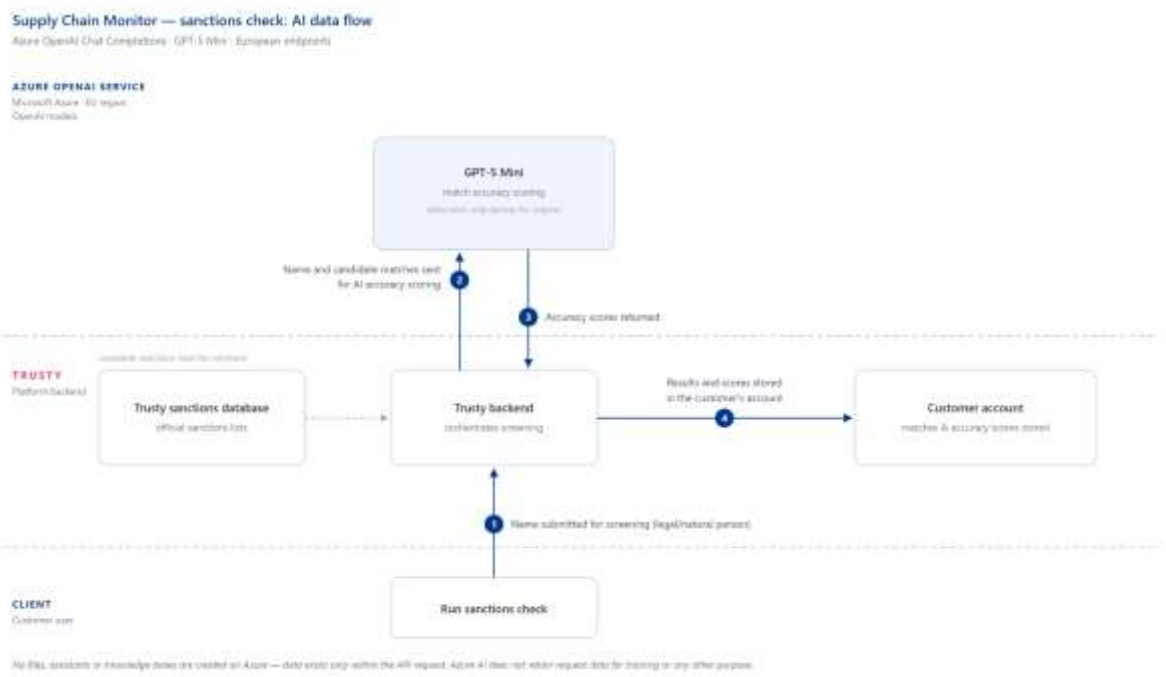
PolicyApp



- AI Model: GPT-5 Mini (GPT-5 Nano for translations)
- Functionality:
    - AI processes client policy documents.
    - Generates concise policy summaries.
    - Translates policy content into the supported languages.
    - **Policy document topic classification**: when a policy source document is uploaded, AI classifies it into compliance topics. The complete document file is transmitted for analysis (including scanned documents, which are read via OCR).
    - **Certifications policy summarization**: the same summarization pipeline is applied to custom policy documents uploaded in the Certifications module.
- **Data handling**: documents are uploaded to Azure AI only for the duration of processing and are automatically deleted afterwards, including when processing fails. No AI assistant or knowledge base persists between requests.

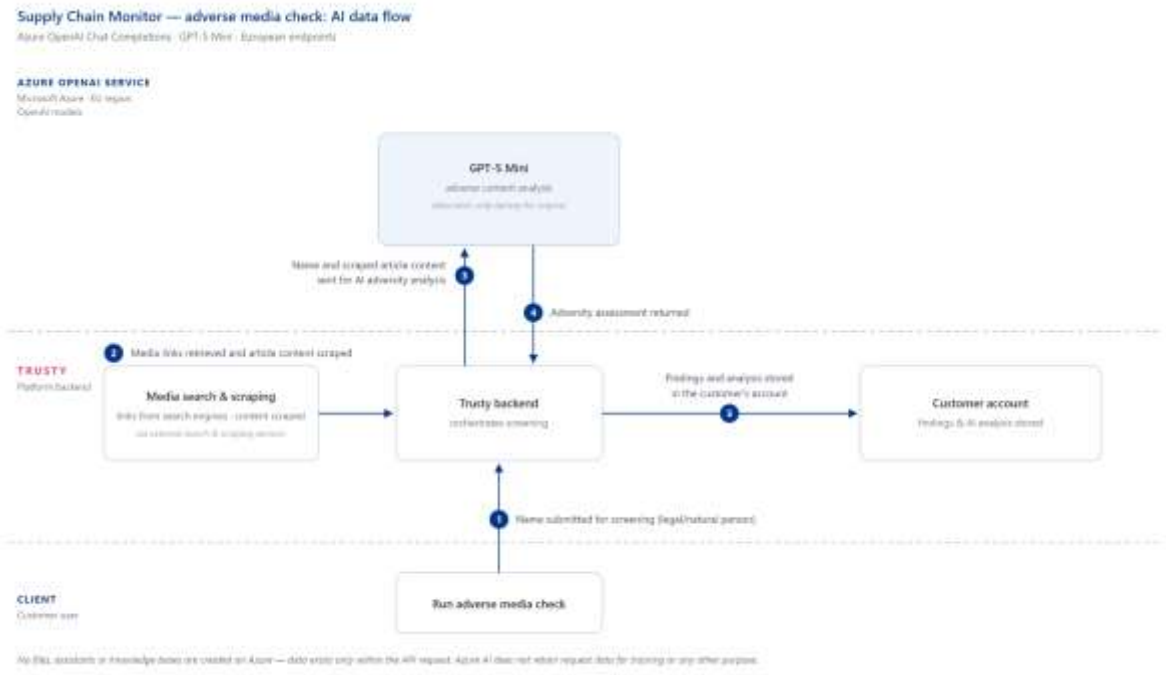
Trusty Supply Chain Monitor

Sanctions Check



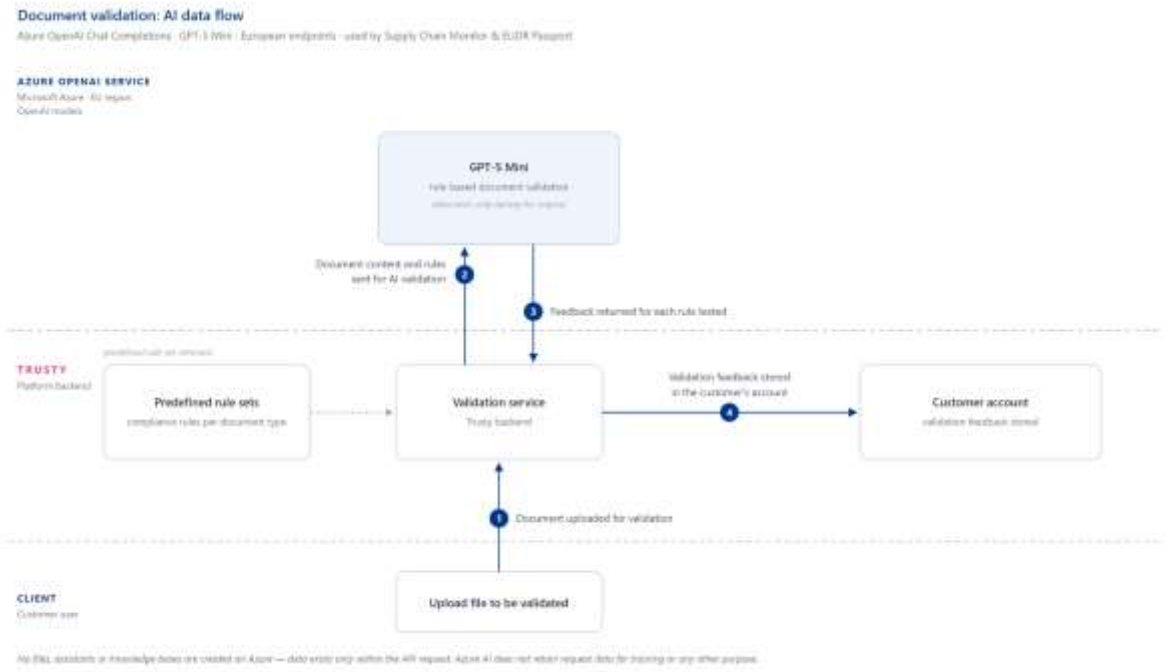
- AI Model GPT-5 Mini
- Functionality:
    - AI compares client-provided names (legal/natural persons) against official sanctions lists.
    - Assesses potential matches and their relevance.

Adverse Media Check



- AI Model: GPT-5 Mini
- Functionality:
    - AI scans the web for media reports on client-provided names (legal/natural persons).
    - Identifies potentially adverse content and provides an analysis.

Document Validation



- AI Model: GPT-5 Mini
- Functionality:
    - AI scans document content for required elements, validates against predefined rule sets, and provides structured feedback on compliance status with specific recommendations for any missing or non-compliant elements.

Quickscreen 360

Quickscreen 360 enables users to perform a rapid welfare check on any company, even without an existing business relationship. It combines insights from our core services — **sanctions screening**, **adverse media analysis**, and **PEPs checks** — to deliver a concise, privacy-conscious risk overview.

All processing is carried out in line with strict data protection standards, with no personal data being retained by the AI provider beyond the session; screening results are stored in the customer's account. Importantly, **PEPs checks do not involve the use of AI**. Only **adverse media** and **sanctions checks** incorporate AI models hosted via Azure AI on European endpoints, ensuring compliance with EU privacy regulations.

For further details on how AI is used in those components, please refer to the dedicated sections on **Adverse Media** and **Sanctions Check**.

EUDR Passport

EUDR Passport provides comprehensive due diligence documentation and compliance verification for companies operating within the European Union Deforestation Regulation framework. It enables users to systematically collect, validate, and manage all required documentation for EUDR compliance, including deforestation risk assessments, supply chain traceability, and regulatory documentation.

The system combines multiple AI-powered validation tools to ensure document completeness and accuracy across various compliance categories — from tax and trade compliance to forest certification and adverse media analysis. All AI processing is conducted using Azure AI models hosted on European endpoints, ensuring full compliance with EU privacy regulations and data protection standards.

Key AI components include specialized document validators for EUDR-specific requirements and adverse media analysis for risk assessment. For detailed information on AI usage within specific validation components, please refer to the dedicated sections on **Document Validation** and **Adverse Media Analysis**.

Platform Help Assistant

The Trusty Compliance Platform includes an in-app help assistant, available from any page, that answers questions about how to use the platform and can perform simple page actions on the user's behalf (for example, opening the relevant form or filter).

- AI Model: GPT-5 Mini
- Functionality:
    - Answers user questions about the current page and platform features, based on Trusty's internal product documentation.
    - Suggests or triggers available page actions to guide the user.
- Data handling:
    - The data transmitted to Azure AI consists of the user's questions, the conversation so far, Trusty's own product documentation, and limited page context (such as the names of available actions and uploaded files). Client business data is not part of the assistant's knowledge base.
    - The conversation exists only for the duration of the session and is not retained after it ends.
    - Messages sent through the separate "contact support" option are delivered to Trusty's support team and stored with the account; that channel does not involve AI.

Security & Compliance

- All data is transmitted using industry-standard encryption to ensure confidentiality and integrity.
- AI usage is fully aligned with European regulations, including GDPR, as models are hosted by Azure AI on European endpoints. This ensures that personal data is processed within the EU, under strict compliance with European privacy standards.
- No client data is retained by the AI provider beyond the processing session; screening results and summaries are stored in the customer's own Trusty account.
- For more information on personal data handling, please refer to our [Data Processing Agreement] and the [CCPA/CPRA Service Provider Contract] for applicable regions.

Provider Privacy Policies

For more detailed information about data privacy, processing, and security related to Azure AI and OpenAI models, we encourage users to review the official privacy policy provided by Microsoft. This policy outlines how data is handled when using the Azure OpenAI Service, including the use of AI models hosted on European endpoints.

For further details, please refer to the following link:

Azure OpenAI Privacy and Data Processing Policy

Trusty AG, Switzerland

July 2026