Magic Cloud

Managed AI Platform

Security, data processing and compliance description

Managed AI Platform

Security, data processing and compliance description

Contents

1. Managed service and division of responsibilities 3
2. Platform security 4
3. Data management and data protection 5
4. Compliance: ISO 27001 and NIS2 6
5. Continuity and disruption situations.....6
6. Sustainability 7

Magic Cloud Oy
Hallituskatu 8A
FI-33200 Tampere

+ 358 10 328 4700
myynti@magiccloud.fi
www.magiccloud.fi

1. Managed service and division of responsibilities

Magic Cloud's managed AI platform provides an environment produced in Finland for AI solutions. The service combines language models, computing capacity, the tools needed to utilise the organisation's own data and user and resource management. The organisation can use AI, for example, for information retrieval, document processing and its own applications without maintaining its own platform infrastructure or worrying about data being transferred outside the organisation or Finland.

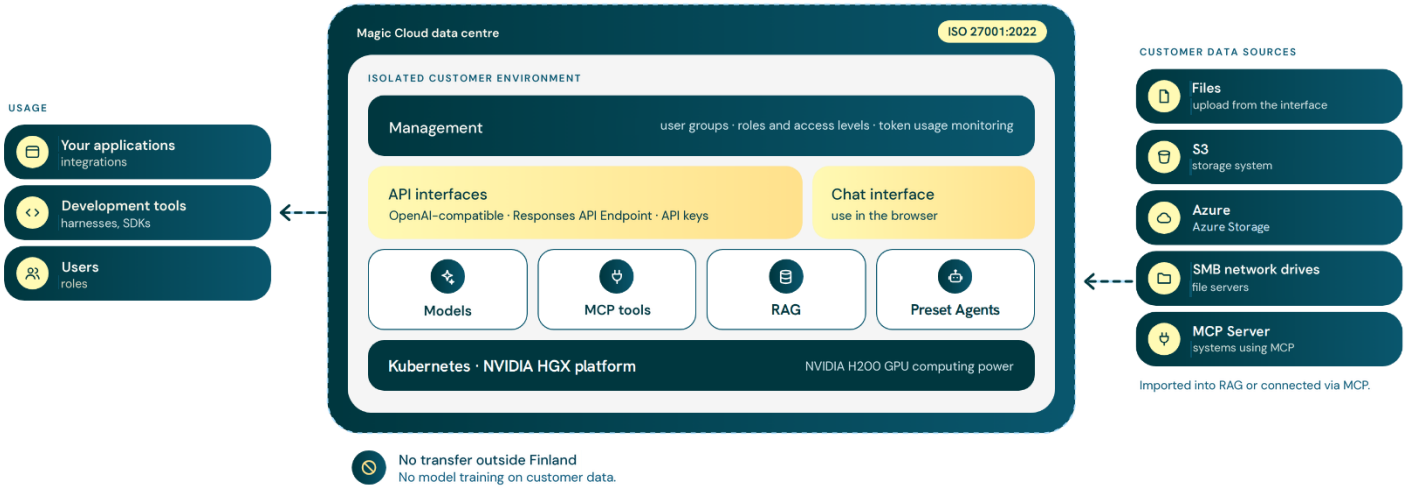
The service is produced from Magic Cloud's own data centres in Finland. Magic Cloud is a 100% Finnish-owned company.

Magic Cloud is responsible for the platform infrastructure, technical maintenance, updates, vulnerability management, model lifecycle management and monitoring of service performance. **The customer** decides on the purposes of use, the data to be processed and the access rights and is responsible for the use of AI in its own operations. A more detailed description and service-specific commitments are defined in the agreement.

Service component	Service description
Models	The service uses AI models pre-trained by various publishers, from which the customer can choose the option suited to its purpose of use. The origin, version and licence terms of the model are taken into account in selection and use. The up-to-date model selection is published on Magic Cloud's website. The customer is responsible for the operation of the model and its suitability for its own use.
Model lifecycle management	Magic Cloud selects, validates and maintains the platform's model library based on customers' use cases and market developments. Each model is validated for quality, performance and security before release. Customers are notified of model changes in advance by email.
RAG	The platform's RAG functionality retrieves information from the customer's data to support the language model's response. Using your own data does not require training the model with the customer's data. A vector database is created in the service from the customer's data, where the information is updated according to the synchronisation interval, depending on the location of the customer's own original data.
MCP	With the platform's MCP (Model Context Protocol) support, external systems can be connected to the AI solution for retrieving information and performing agreed actions. Access control is implemented using either OAuth tokens or an API key.

Service component	Service description
Built-in Chat	The platform's built-in Chat can be used to make queries and save conversations related to the tools and data linked to the platform. Each user has a Chat interface where queries can be saved.

Architecture



2. Platform security

The platform's technical protection is based on the logical isolation of customer environments. Magic Cloud takes care of platform updates, vulnerability management and service monitoring as part of technical maintenance.

Security control	Function
Isolation	Customer environments are logically isolated from one another.
Platform access control	The customer defines user-, group- and resource-specific access rights to models, data and tools. The permissions of API keys can be restricted according to the purpose of use.
API keys	The service has restricted API keys for the use of models, RAG, MCP and agents, on a per-user, per-group or per-environment basis.

Security control	Function
Vulnerability management	Vulnerability management is carried out as part of service maintenance. Magic Cloud monitors public security bulletins and identified vulnerabilities and takes the necessary measures to remediate them.
Updates	Magic Cloud performs the necessary updates (from the infrastructure level to the application level) to ensure the quality, performance and security of the platform.

3. Data management and data protection

Customer data is processed only in the customer's isolated environment in Finland and is not used for training AI models.

Service component	Data management
Models	The AI platform and the language models connected to it operate in Magic Cloud's own environment located in Finland. Customer data, user inputs and model responses are not used for training or fine-tuning models. Data is also not passed on to external model services.
Chat	Queries and conversations in the built-in Chat are saved in the user's personal chat tool. The customer and the user can delete and add conversations.
API keys	Prompts and queries used in third-party tools are not stored on the platform when the platform is used through API interfaces.
RAG	The customer manages the data it has stored on the platform for information retrieval (RAG data). Deleting a RAG resource or a customer environment covers both the data stored in it and the information created for information retrieval. Deletion does not affect the original data in the source system.
Backups	Tool usage, users, usage monitoring and chat conversations related to the customer environment are backed up.

When the customer acts as the controller, Magic Cloud processes personal data on behalf of the customer in accordance with the data processing agreement and the customer's written instructions. The agreement defines the content and terms of the processing and identifies the sub-processors participating in the service. The customer is responsible for the legal basis of

the processing and for ensuring that the personal data is necessary for the purpose of use. Magic Cloud assists the customer in implementing data subjects' rights and, where necessary, in data protection impact assessments in accordance with the data processing agreement and the General Data Protection Regulation (GDPR).

4. Compliance: ISO 27001 and NIS2

ISO/IEC 27001:2022 and information security management

Magic Cloud's ISO/IEC 27001:2022-certified information security management system covers data centre and cloud services, including their supporting functions and processes. The maintenance and development of information security are guided by risk assessment and treatment. The operation of the management system is evaluated through regular internal audits, management reviews and audits by an independent certification body.

NIS2

Magic Cloud's information security management, continuity procedures and incident handling support the customer's risk management and supplier assessment. They also support meeting the requirements of the NIS2 regulation where the customer falls within its scope. Magic Cloud and the customer are each responsible for the statutory obligations applicable to their own operations.

AI Act and assessment of use cases

The requirements of the EU AI Act are determined by the purpose of use, the risk category and the roles of the parties. Magic Cloud is responsible for its obligations applicable to providing the platform service. The customer assesses the requirements related to its own use case and takes care of the onboarding of its personnel, the development of AI skills, and the human oversight and transparency of AI use required by the use case.

5. Continuity and disruption situations

The critical infrastructure of the data centres is duplicated. A more detailed description of our data centre can be found here. In disruption situations, Magic Cloud limits the effects of the disruption, takes care of restoring the service and informs the customer in accordance with the agreed operating model and applicable legislation. Deviations and corrective actions are documented.

Magic Cloud notifies the controller of a personal data breach without undue delay and where possible within 72 hours of the controller becoming aware of the breach. In accordance with the NIS2 Directive, the initial notification is made within 24 hours of the controller becoming aware

of the breach. The applicable obligations of the Cybersecurity Act are also followed when reporting significant incidents and cyber threats.

Magic Cloud's technical support service serves customers on weekdays between 8:00 and 16:00.

6. Sustainability

Magic Cloud uses 100% renewable electricity and develops the energy efficiency of its service production as well as the responsible lifecycle management of its equipment. Environmental work is guided by an Ekokompassi-certified environmental system, the achievement of whose targets is monitored regularly. Operations are assessed in independent external audits. The targeting of development measures is supported by an annual carbon footprint calculation, carried out by an external party in accordance with the GHG Protocol standard.

The customer can influence the resource requirements of AI use by choosing a model that matches the demands of the task and by sizing usage according to need. The customer can also use the sustainability information published by Magic Cloud in its own reporting and to support its procurement decisions. More detailed information on environmental work and the results of the carbon footprint calculation is provided on request.