Personal Data Processing Policy for Integrations via API and MCP

1. Identity and Contact Details of the Controller

The controller of personal data is:

Mergado technologies, s. r. o. with its registered office at Pavlovská 12, 623 00 Brno, Czech Republic, Company ID No.: 03570061, registered in the Commercial Register maintained by the Regional Court in Brno, Section C, Insert 85012, email: mergado@mergado.com, telephone: +420 608 44 00 67

(hereinafter referred to as the “controller”)

The controller has not appointed a Data Protection Officer.

2. Scope and Purpose of This Document

This Policy governs the processing of personal data in connection with the integration of the Mergado service with external third-party tools through an application programming interface (API) or through technologies such as MCP (Model Context Protocol) or similar integration mechanisms.

This concerns in particular integrations with:

- artificial intelligence tools (e.g. Claude by Anthropic, ChatGPT by OpenAI),
- automation and integration platforms (e.g. Gumloop, Make.com, Zapier, and similar),
- other external services that access the Mergado service on behalf of the User on the basis of the User’s authorization.

This Policy supplements the general information on the processing of personal data set out in the Mergado Terms of Use and, in the event of any conflict, the provisions of this Policy shall take precedence with respect to integrations via API and MCP.

3. Data Processed within Integrations

3.1 Data Received from External Tools

When an integration is used, the controller may process in particular:

- parameters of requests sent by the external tool (e.g. project identifiers, e-shop identifiers, rule identifiers, queries, filters),
- authentication data (e.g. OAuth tokens or other access credentials).

3.2 Data Provided to External Tools

In response to requests, the controller may provide in particular:

- product data (e.g. names, prices, availability),
- product feed data,
- results of analyses, diagnostics, and audits,
- rule configuration and status,

- information about the User's projects and accounts.

3.3 Data Not Processed

Within these integrations, the controller does not process:

- the content of conversations between the User and the external AI tool,
- chat histories, their summaries, or AI tool memory,
- files uploaded by the User to the external tool,
- any data not expressly transmitted as part of a specific request.

The controller does not request or actively obtain any data from the external AI tool's environment beyond the parameters of individual requests.

4. Purpose and Legal Basis for Processing

Personal data are processed exclusively for the purpose of ensuring the functionality of the integration and providing Mergado services through external tools.

The legal basis for processing is:

- performance of the contract between the User and the controller within the meaning of Article 6(1)(b) of the GDPR,
- the legitimate interests of the controller within the meaning of Article 6(1)(f) of the GDPR, in particular ensuring the security, operation, technical stability, and protection of the service against misuse,
- the User's consent within the meaning of Article 6(1)(a) of the GDPR, expressed through the authorization of the integration (e.g. OAuth), to the extent that the User has actively permitted the connection of a specific external tool.

The controller does not carry out automated individual decision-making within the meaning of Article 22 of the GDPR in the context of integrations.

5. Data Minimization Principle

The controller processes only such data as are necessary for performing the specific operation requested by the User through the external tool.

No excess data are collected, nor is information obtained beyond the parameters of a specific request. The controller does not access data from the external AI tool beyond those transmitted as part of a specific request.

6. Transfer of Data to Third Parties

6.1 Recipient within the Integration

Data processed within integrations are transferred exclusively to the external tool that initiated the request and to which the User has granted authorization.

6.2 General Restrictions

The controller:

- does not sell personal data,

- does not rent personal data,
- does not use data obtained from API/MCP communications for targeted advertising or profiling,
- does not use data obtained from API/MCP communications for training its own artificial intelligence models,
- does not transfer data from API/MCP communications to providers of language models (e.g. OpenAI, Anthropic) for the purposes of training their models.

6.3 Processors

Data may be further processed by processors listed in the Terms of Use, to the extent necessary for ensuring the operation of the service (in particular providers of infrastructure, hosting, and technical support).

6.4 Internal Use of Language Models within the Integration

At present, the controller does not make the content of requests received through API/MCP integrations available to any providers of language models when processing such requests. Should functionality be introduced in the future that requires such processing (e.g. generating recommendations using a server-side LLM), this Policy will be updated and the User will be informed of the change in the manner set out in Article 12.

7. Data Retention Periods

- **Request records (API/MCP communication logs):** retained for 90 days from the date of the request, exclusively for the purposes of security, audit, resolution of technical issues, and protection of the controller's rights. For operational and performance statistics (e.g. call counts, usage of individual functions, performance metrics), such records may be aggregated within the stated retention period.
- **Authentication data (OAuth tokens and similar):** retained for the duration of their validity. Upon revocation of access by the User or upon expiry, they are deleted without undue delay.

Upon expiry of the stated periods, data are deleted or anonymized.

8. Data Security

The controller has implemented appropriate technical and organizational measures to protect personal data processed within integrations, in particular:

- encrypted communications via HTTPS / TLS,
- authentication through the OAuth 2.1 protocol using the PKCE (Proof Key for Code Exchange) mechanism,
- secure storage of access credentials and tokens (encryption at rest),
- access control on the principle of least privilege,
- rate limiting as protection against misuse,
- monitoring, audit logging, and anomaly detection.

9. Rights of the Data Subject

Under the conditions set out in the GDPR, the User has in particular the right:

- of access to personal data,
- to rectification of inaccurate personal data,
- to erasure of personal data (“right to be forgotten”),
- to restriction of processing,
- to data portability,
- to object to processing,
- to withdraw consent given at any time (e.g. by disconnecting the integration — see Article 10).

The User also has the right to lodge a complaint with the supervisory authority, which in the Czech Republic is the Office for Personal Data Protection (www.uoou.cz).

More detailed information on the rights of data subjects is set out in the Terms of Use, section “Information on the Processing of Personal Data”.

10. Right to Revoke Access

The User may terminate the connection with an external tool at any time:

- in the Mergado service interface (integrations / connected applications section),
- in the external tool’s interface (where the tool permits this),
- in the settings of the User’s account with the authorization provider (e.g. Google, where relevant).

Upon revocation of access, further processing of data within the given integration ceases immediately. Historical request records are retained for the period set out in Article 7.

11. Security Contact and Vulnerability Reporting

For security inquiries or to report vulnerabilities, the User may contact the controller at: security@mergado.com

Vulnerability reports are investigated with due diligence. The controller undertakes to respond to reports within a reasonable period, generally within 5 business days of receipt.

For general user support, the following address should be used: mergado@mergado.com

12. Amendments to This Policy

This Policy may be updated from time to time, in particular as a result of changes in legislation, technical conditions of integrations, or the scope of services provided.

The current version is always available on the controller’s website. Users will be informed of material changes in the manner set out in the Terms of Use.

13. Compliance with the Terms of AI and Integration Platform Providers

The controller undertakes to provide integrations in compliance with the terms of individual providers, in particular:

- Anthropic Usage Policy (for integration with the Claude service),
- OpenAI Usage Policies (for integration with the ChatGPT service),
- the terms of other integration platforms (e.g. Gumloop, Make.com), where applicable.