GAIA Platform Privacy Policy

This Privacy Policy describes how the GAIA Platform, operated by UBITECH, accesses, collects, uses, stores, and shares information, and the controls available to users regarding their personal data.

This Privacy Policy describes how the GAIA Platform, operated by UBITECH, accesses, collects, uses, stores, and shares information, and the controls available to users regarding their personal data.

GAIA is a governed, enterprise operating layer for designing, running, and governing AI agents and applications. It is designed for CIOs, CTOs, platform teams, and delivery teams operating in regulated, risk-sensitive, or mission-critical environments.

For the purposes of applicable data protection legislation, including Regulation (EU) 2016/679 (GDPR), UBITECH acts as the data controller for personal data processed at the platform level. The customer organization deploying a GAIA tenant may act as a separate or joint data controller for personal data it causes to be processed within that tenant. Enterprise customers are responsible for ensuring that any personal data uploaded or processed via the Platform in their tenant has an appropriate legal basis and data protection safeguards, as further governed by the relevant Data Processing Agreement.

This Policy should be read together with the applicable master service agreement, data processing addendum, and terms of use governing your organization's use of the Platform.

1. Data Collected

The Platform processes information necessary to build, govern, evaluate, and scale enterprise AI workflows, agents, and applications.

- Account and Profile Information: Corporate email addresses, user identifiers, login credentials such as Single Sign-On, and role configurations provided during account setup and administration.
- Enterprise Data and Inputs: Contextual knowledge bases, document folders, enterprise data sources, and user interaction layers securely connected to the Platform by the customer organization. Customer organizations are responsible for ensuring any personal data within these sources has an appropriate legal basis for processing.
- Runtime and Operational Data: Execution logs, agent behavior records, runtime decisions, and lifecycle evidence generated during the operation of AI agents to support complete auditability.
- Usage and Technical Data: Browser type, device information, IP addresses, session identifiers, and platform interaction logs used solely for platform security, diagnostics, and performance monitoring.
- Personal Data Minimisation: No personal data submission is required to receive responses or execute workflows on the Platform. Users and administrators are encouraged to avoid uploading unnecessary personal information. Any personal data voluntarily submitted or contained within connected enterprise data sources is processed strictly as functional input to execute requested AI workflows.

2. Legal Basis for Processing

Where the GDPR or other applicable data protection legislation applies, we rely on the following legal bases for processing personal data.

- Contractual necessity: Processing account and profile data is necessary to provide the Platform services under our agreement with the customer organization.
- Legitimate interests: Processing runtime, operational, and technical data helps maintain the security, integrity, and performance of the Platform.
- Legal obligation: Data may be disclosed where required by applicable law or binding legal order.
- Consent: Where consent is the legal basis for a specific processing activity, we will obtain it separately and record it. You may withdraw consent at any time without affecting the lawfulness of prior processing.

3. Usage and Storage

We use, secure, and store information exclusively to provide runtime control, risk governance, and multi-model AI operations.

- Purpose of Usage: Data is used to design and orchestrate AI agents, run evaluations, enforce policy controls, and maintain system visibility. Data processed by the Platform is strictly isolated, remains within the designated cloud storage environment, and is never used to train public or third-party artificial intelligence models.

- Security Measures: We implement technical and organisational security measures including data encryption in transit using TLS 1.2 or higher, encryption at rest using AES-256 or equivalent, strict access controls, policy enforcement, and risk-management workflows.
- Storage, Localisation, and Retention: Operational, governance, evaluation, and lifecycle evidence data is stored within designated cloud storage environments located inside the European Union and is not transferred outside the EU unless explicitly required by customer configuration and subject to appropriate transfer mechanisms under Chapter V of the GDPR, such as Standard Contractual Clauses.
- Session Data: Temporary runtime execution data is cleared from browser and runtime memory upon session termination.
- Audit and Governance Logs: Audit trails, regression checks, and governance logs are stored securely for up to 20 days, or in accordance with customer compliance configurations, solely to maintain auditability and prevent misuse. Retention periods for specific categories of data are set out in the applicable Data Processing Agreement.

4. Data Sharing

We do not sell personal data. Data sharing and disclosure are strictly limited to the following categories of recipients to fulfil platform functionality.

- Enterprise Control: Data is shared with the customer organization managing the GAIA Platform tenant, such as enterprise administrators, CIOs, and platform teams, to maintain internal governance.
- Authorised Multi-Model Providers: When executing agent workflows, data inputs may be securely transmitted to designated LLM or AI infrastructure providers configured explicitly by the customer organization. These third parties act strictly as data processors under enterprise-grade data protection terms, and UBITECH ensures appropriate data processing agreements or equivalent safeguards are in place with all such sub-processors.
- Service Providers and Sub-processors: We may engage trusted third-party vendors such as cloud infrastructure providers and monitoring services that process data on our behalf solely to support delivery of the Platform. All sub-processors are bound by contractual data protection obligations no less protective than those in this Policy.
- Legal and Regulatory Compliance: Data may be disclosed if required by law, regulation, or a binding legal order, or to protect the safety and security of the Platform.

5. Cookies and Tracking Technologies

The Platform may use session cookies and similar technologies to maintain user sessions, support authentication, and ensure the security and proper functioning of the Platform.

We do not use cookies for advertising or cross-site tracking purposes. Strictly necessary cookies are deployed on the basis of our legitimate interest in delivering a secure and functional service. If we introduce any non-essential cookies in the future, we will obtain consent before setting them and update this Policy accordingly.

6. User Controls and Data Subject Rights

Depending on your jurisdiction, you may have rights over your personal information.

- Right of Access: You may request a copy of the personal data we hold about you.
- Right to Rectification: You may review, modify, or update account and profile information through the Platform user settings or by contacting your organization's tenant administrator.
- Right to Erasure: You may request deletion of your personal data, subject to any legal retention obligations.
- Right to Restriction: You may request that we restrict processing of your personal data in certain circumstances.
- Right to Data Portability: Where processing is based on contract or consent and carried out by automated means, you may request your personal data in a structured, commonly used, machine-readable format.
- Right to Object: Where processing is based on legitimate interests, you may object. We will then cease processing unless we can demonstrate compelling legitimate grounds that override your interests.
- Rights Related to Automated Decision-Making: No automated decision-making or user profiling that produces legal or similarly significant effects takes place at the Platform level unless explicitly designed, configured, and governed by the customer organization.
- Control Over Data Sharing: Enterprise administrators control which data sources, document folders, and third-party model providers are connected to the Platform.
- Right to Lodge a Complaint: You may lodge a complaint with your local supervisory authority. For users in Greece, this is the Hellenic Data Protection Authority at www.dpa.gr.

7. Data Deletion Requests

Because GAIA operates as an enterprise platform, requests regarding data stored within a specific organization's tenant should generally be directed to that organization's data administrator first.

For platform-level inquiries or direct deletion requests, email info@ubitech.eu with the subject line "GAIA Platform - Data Deletion Request" and include your login ID, email address, or corporate tenant details so we can locate and process associated data.

- We will respond within the timeframe required by applicable law, no later than one month under the GDPR, with a possible extension of two further months for complex requests.
- We will confirm receipt of your request within a reasonable timeframe.
- We will coordinate with the necessary technical parties to delete attributable personal data unless we are legally required or contractually bound to retain it.
- We will provide formal confirmation once deletion has been successfully completed.

8. Data Breach Notification

In the event of a personal data breach likely to result in a risk to the rights and freedoms of natural persons, UBITECH will notify the relevant supervisory authority within 72 hours of becoming aware of the breach, in accordance with Article 33 of the GDPR.

Where a breach is likely to result in a high risk to individuals, affected individuals will also be notified without undue delay unless an exemption applies. Customer organizations will be informed promptly so they can fulfil their own notification obligations.

9. Children's Privacy

The GAIA Platform is an enterprise software solution intended solely for use by organizations and their authorized personnel. It is not directed at or intended for use by individuals under the age of 16.

We do not knowingly collect personal data from children. If you become aware that a child has provided personal data through the Platform, contact info@ubitech.eu so that we may take appropriate steps.

10. Microsoft Marketplace

GAIA is published on the Microsoft Azure Marketplace. By acquiring the Platform through Microsoft's commercial marketplace, you acknowledge that Microsoft may collect and process certain transaction and usage data in accordance with its own privacy policies and marketplace terms.

UBITECH is the publisher and operator of the Platform. Microsoft acts solely as a marketplace intermediary and is not a data controller in respect of your use of the Platform itself. We encourage you to review Microsoft's Privacy Statement at https://privacy.microsoft.com for details of its data practices.

11. Additional Information

This Privacy Policy complements the master service agreements, data protection addendums, and terms of use of UBITECH and the respective customer organizations using the GAIA Platform.

In the event of any conflict between this Policy and the applicable data processing addendum, the data processing addendum shall prevail.

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in law, our data practices, or Platform features.

When we make material changes, we will notify customer organizations and, where practicable, individual users via email or a prominent notice within the Platform. The date of the most recent revision is indicated on this page. Continued use of the Platform after such notification constitutes acceptance of the revised Policy.

13. Contact

If you have questions about this Privacy Policy or wish to exercise rights under applicable data protection legislation, contact info@ubitech.eu with the subject line "GAIA Platform - Privacy Inquiry".

Data Protection Officer contact details, where applicable, will be provided through UBITECH's official contact channel.