

Privacy Policy

1. General Information

This Privacy Policy explains what personal data we (Ariadne Industries GmbH, Anton-Huber-Strasse 20, 73430 Aalen, email: info@ariadneanyverse.de – referred to as “we” or “us”) collect in connection with our website and our AI application “Ariadne’s Advanced Agents,” and for what purposes this data is processed.

Important note: Please do not enter sensitive or personal data into our AI application unless you are certain you have the rights to do so. You are solely responsible for the content you upload or enter.

2. Definitions and Legal Bases

- **Personal data** means any information relating to an identified or identifiable natural person (e.g., name, email address).
 - We process your data in compliance with the provisions of the General Data Protection Regulation (GDPR) and national laws.
 - The most relevant legal bases are:
 - **Art. 6(1)(b) GDPR** (fulfillment of contract/pre-contractual measures)
 - **Art. 6(1)(a) GDPR** (consent), for example if you explicitly allow us to share data with third parties
 - **Art. 6(1)(f) GDPR** (legitimate interest), for instance for IT security
-

3. Controller

The controller responsible for data processing is:

Ariadne Industries GmbH

Anton-Huber-Strasse 20

73430 Aalen

Email: info@ariadneanyverse.de

You can direct any data protection inquiries to the above contact details.

4. Hosting and Server Log Files

Our website is hosted on servers operated by Uberspace and Hetzner Online GmbH (Germany). Each time you visit our websites, the following data is collected automatically:

- IP address
- Date and time of access
- Browser type/browser version, operating system
- Referrer URL (the page visited before)

We store these log files to ensure smooth operation and for error analysis (Art. 6(1)(f) GDPR).

Details about the hosting providers:

- Jonas Pasche “Uberspace,” Kaiserstr. 15, 55116 Mainz
- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen

Data Processing on Our Behalf

We have concluded a Data Processing Agreement (DPA) with each of the above providers as required by data protection law. This ensures that any personal data of our website visitors is processed solely in accordance with our instructions and in compliance with the GDPR.

5. SSL/TLS Encryption

Our website uses SSL/TLS encryption to protect transmitted data from unauthorized access. You can recognize this by the “https://” in the address bar and the lock icon in your browser.

6. Registration, User Account, and Application Data

6.1 Registration

You can register with a freely chosen username and password. At a minimum, we collect the following:

- **Login data** (username, password hash)

6.2 Chat Histories and Application Data

In our AI application, we store your chat histories and other content (e.g., uploaded files, texts, documents) in a **user-specific isolated database**. This data is assigned to your profile and not mixed with other users’ data. You can delete your content at any time via the user interface (UI).

6.3 Encryption of Your Application Data

All application and chat data are stored **server-side in encrypted form (“data at rest”)**.

- We use **gocryptfs** with **AES-256 encryption in GCM mode**.
- Encryption keys are stored exclusively on our servers in a secured key store and are not accessible to unauthorized parties.
- The encryption covers all files and database files associated with your user account.
- During active processing (e.g., while you are using the app) data are temporarily decrypted; transmission is protected by **TLS**.

This provides an additional layer of protection against unauthorized access or physical loss of storage media. You can still delete all your data at any time via the UI.

6.4 No Use of User Data for Training or Advertising Purposes

We do not use any of the data you enter (e.g., texts, documents) for our own AI training or for advertising. No content analysis or profiling takes place. Each user has an **isolated data area**,

strictly separate from other users' data. This ensures that only you have access to your content (except in cases where you explicitly grant us access for support or maintenance reasons).

6.5 Logging of Technical Metadata

To ensure a secure and reliable operation, we collect **technical log data** exclusively for error analysis and system stability. This includes:

- **Login and session information** (time of login/logout, session IDs)
- **Request frequency** (e.g., number of requests made)
- **Error messages** or similar system events (for troubleshooting)

We use these data solely to identify technical issues, optimize system stability, and generate **anonymous usage statistics** (e.g., daily user count). We do not perform any personal or content analysis.

6.6 Technical and Organizational Measures (TOMs)

We implement appropriate TOMs to protect your data from loss, misuse, or unauthorized access. These measures include:

- **SSL/TLS encryption** for data transfer
 - **Isolated databases** for each user
 - **Strict access restrictions** for server and support staff
 - **Regular security updates** and **backups**
 - A **convenient deletion option** for all data you have entered
-

7. Choice of AI Models and Data Processing

In our “Ariadne’s Advanced Agents” application, you can choose from different AI models. Depending on the model, server locations and data processing details vary.

7.1 Using OpenAI (USA)

- **Description:** If you decide to use an OpenAI model (e.g., GPT models), your chat inputs will be transferred to servers in the USA.
- **No training usage:** We have configured OpenAI not to use your inputs for training purposes.
- **Legal basis and safeguards:**
 - We have accepted OpenAI’s [Data Processing Addendum \(DPA\)](#) for EU/EEA countries, which essentially functions as a data processing agreement and aims to ensure GDPR compliance.
 - Transfer to the USA takes place based on appropriate safeguards (e.g., Standard Contractual Clauses) and your consent to use US-based models (Art. 6(1)(a) GDPR). Please note that data protection levels in the USA may differ from those in the EU.

7.2 Using Ubicloud (Germany)

- **Description:** As an alternative, you can choose Ubicloud models, hosted on **German Hetzner servers**.

- **No data storage of user inputs:** According to Ubicloud, user inputs are not used for training, logged, or permanently stored.
- **Data processing agreement:** We have also concluded a data processing agreement with Ubicloud, ensuring GDPR compliance on German servers.

7.3 Processing of Images by Mistral AI (Sweden)

- **Description:** When you upload individual images—or when images are embedded in a document—these files are sent to **Mistral AI** for AI processing. The processing takes place on servers located in **Sweden** (within the EU).
- **Purpose of processing:** Image analysis, text extraction (OCR), or other AI-based image processing as part of the feature you requested.
- **Retention period:** Mistral AI keeps **log and system data** related to each request for up to **30 days** for debugging and security purposes; a zero-data-retention mode is currently not available.
- **Legal basis:** The transfer is necessary for **contract performance** / provision of the requested function (Art. 6 (1)(b) GDPR) and is also based on our **legitimate interest** in operating stable and secure AI features (Art. 6 (1)(f) GDPR).
- **Safeguards:** All data are processed exclusively within the EU. Mistral AI is contractually bound to GDPR compliance and applies state-of-the-art technical and organizational security measures to protect your data.

Your responsibility: You can decide at any time which AI models to use within “Ariadne’s Advanced Agents.” Please be aware that choosing the US-based OpenAI models involves data transfers to a third country (USA).

8. Processing of Customer and Contract Data

If you use our services for a fee or enter into a contract (see our T&C https://www.ariadneanyverse.de/T&C_english.pdf), we process the following data for contract fulfillment:

- **Name/Company, address, payment data (if applicable)**
- **Contact details** (email, phone number)
- **Contract and order details** (e.g., subscription plan)

We store this data as long as needed for its purpose or as required by law (e.g., accounting).

9. Payment Processing (Stripe)

9.1 Payment Transactions

For payments (e.g., subscriptions to our AI application), we use the Stripe service. If you pay by credit card or other Stripe-supported methods, relevant payment data (e.g., card number, expiration date, invoice amount) is transmitted directly to Stripe.

9.2 Data Processing by Stripe

- Stripe, Inc. is based in the USA. Therefore, your data may be transferred to the USA.
- We have agreed to Standard Contractual Clauses (SCCs) or other contractual safeguards with Stripe (Art. 46 GDPR).
- Legal basis: **Fulfillment of contract** (Art. 6(1)(b) GDPR).

For further details, see Stripe's Privacy Policy: <https://stripe.com/de/privacy>.

10. Appointment Scheduling: Calendly and Google Meet

10.1 Calendly

If you schedule an appointment (e.g., a demo) via Calendly, the data you provide (name, email, etc.) is stored on Calendly Inc. servers in the USA. Standard Contractual Clauses or the Data Privacy Framework also apply here.

For more info, see Calendly's privacy notice: <https://calendly.com/legal/privacy-notice>

10.2 Google Meet

Appointments may take place via Google Meet. As soon as you join a Google Meet link, personal data (e.g., video/audio content) may be transferred to Google (USA).

- Legal basis: **Consent** (Art. 6(1)(a) GDPR) or **Contract fulfillment** (Art. 6(1)(b) GDPR).
 - Privacy Policy: <https://policies.google.com/privacy>
-

11. Cookies

We use cookies and similar technologies to provide certain features (e.g., login) and ensure stability.

- **Necessary cookies** are stored based on Art. 6(1)(f) GDPR (legitimate interest in a functional website).
- **Other cookies** (e.g., for analytics) are placed only with your consent (Art. 6(1)(a) GDPR).

You can manage (delete/decline) cookies in your browser settings.

12. Social Media Profiles

We maintain public profiles on social networks (e.g., Instagram, X/Twitter). When you visit or interact with these platforms, the respective platform's privacy policies apply. We have no direct influence on their data processing.

13. Storage Period and Deletion

We store your personal data only as long as necessary for its respective purpose or as required by law (e.g., commercial and tax regulations). Afterward, the data is either deleted or anonymized.

14. Your Rights

You have the following rights at any time:

- **Access** to your stored data (Art. 15 GDPR)
- **Rectification** of incorrect data (Art. 16 GDPR)
- **Erasure** (Art. 17 GDPR), unless legal requirements prevent it
- **Restriction** of processing (Art. 18 GDPR)
- **Data portability** (Art. 20 GDPR)
- **Objection** to certain data processing (Art. 21 GDPR)
- **Withdrawal** of your consent (Art. 7(3) GDPR) with effect for the future

You also have the right to file a complaint with the competent supervisory authority if you believe your data protection rights have been violated.

15. Changes to This Privacy Policy

We may update this policy from time to time to keep it current. We will inform you of any significant changes, e.g., by email or upon your next login.

(Effective as of February 23, 2025)