White Paper Data Security and Privacy Compliance

Data Security and Privacy Compliance

ATLAS.ti enables the world's leading universities and companies to analyze their data and turn it into qualitive insights. As we process millions of valuable and sensitive data points on a daily basis, we take data security and privacy compliance very seriously and attach utmost importance to safeguarding the personal data we process on behalf of our clients. ATLAS.ti implemented a comprehensive information security and data protection management system to ensure both the security of the data processed with ATLAS.ti Web and full compliance with all relevant privacy laws and regulations, including GDPR, CCPA, HIPAA and LGPD.

Analyzed Data

With ATLAS.ti the users can analyze almost any kind of data, including personal data. Such data is processed by ATLAS.ti as a data processor, on instruction of our clients. Such data processing by ATLAS.ti is subject to our Data Processing Agreement (in accordance with Art. 28 GDPR).

User Data

Users of ATLAS.ti Web provide personal data (like their name and email address) to create an account and to use ATLAS.ti Web. This user data is processed by ATLAS.ti as controller to provide our software and services to our clients. The processing of user data is described in our Privacy Policy. Such data may be processed outside of the EU, based on appropriate safeguards (EU Standard Contractual Clauses).

High Security Data Centers

All data that is handled and processed through ATLAS.ti Web is fully secured against unauthorized access. All data is fully encrypted, managed and stored by SOC-compliant data center providers with all relevant ISOI certifications, including, but not limited to, ISO 27001 and ISO 27018

Hosting in Germany

ATLAS.ti Web is hosted with Amazon Web Services in Germany. The data processed via ATLAS.ti Web by ATLAS.ti as a data processor is processed in the EU only, no data is transferred to third countries outside of the EU.

Sub-Processors in Germany

We are using an external service provider, based in Germany, for support and maintenance of ATLAS.ti Web. In addition, we are using another external service provider, also based in Germany, for hosting and operation of ATLAS.ti Web. The hosting and operations service provider uses the Amazon Web Services data center region Germany (Frankfurt) as hosting provider.

Data Security

ATLAS.ti implemented industry-standard intrusion prevention and detection systems and data loss prevention systems to ensure the security of the data processed with ATLAS.ti Web.

ATLAS.ti implemented a comprehensive framework of security policies, including password requirements, a detailed backup policy and regularly tested business continuity processes. ATLAS.ti implemented a role-based authorization concept on a strict "need to know" basis that ensures that employees receive access rights to applications and data depending on their respective area of responsibility and, if necessary, on a project basis.

All IT systems used by ATLAS.ti for our clients are multi-client capable. The logical assignment of the data processed on behalf of a customer to the respective client and thus the logical separation of the data is always ensured.

Please find a detailed overview of the technical and organizational measures of data security we implemented in our Data Processing Agreement.

AI Data Security and Privacy at ATLAS.ti

At ATLAS.ti, we are committed to building trust by protecting your data and privacy when using our AI-powered features like AI Coding, AI Summaries, or AI Code Suggestions.

Building trust through data protection with OpenAI

We understand that privacy and security are top concerns when using our AI features. That's why we are committed to safeguarding your data through rigorous protections and are fully transparent about how we leverage the power of OpenAI's GPT models. Our multi-layered security approach provides peace of mind knowing your data is in good hands.

Our approach to data protection

- Military-grade Encryption
  Your data is encrypted in transit and at rest using 256-bit AES encryption, the same as militaries worldwide.
- Compliance with GDPR
  We comply with key global data protection regulations, further strengthening our commitment to your data's security.
- No AI Model Training
  None of your data is ever used to train or improve AI models. Your data remains private and isolated.
- Isolated Environments
  Open AI's models run in secure, isolated environments completely separate from your actual data. There is no commingling.
- Minimal Data Collection
  Only the bare essential data required to deliver our AI services is collected. Rest assured, we are committed to minimal data collection.
- Third-party Auditing
  Independent firms audit OpenAI's practices annually to ensure alignment with industry best practices.

FAQ

- What artificial intelligence (AI) technology are you using?
  We are using OpenAI's GPT models through an API to deliver better results to our customers if and insofar our customers are choosing to leverage OpenAI-powered features like AI Coding, AI Summaries, or AI Code Suggestions.
- Are you always using OpenAI technology in your software?
  No, we will only employ specific AI features upon your request through an opt-in or other sign-up process. Additional fees might apply.
- Are you using my personal data for the AI analysis?
  The AI will process all data that is fed into it in order to run an analysis. We have concluded a Data Processing Agreement, including the Standard Contractual Clauses (SCC) with OpenAI, that ensures the safety of your personal data.

- Is my personal data safe?
  We have concluded a Data Processing Agreement including the Standard Contractual Clauses (SCC) with OpenAI that ensures the safety of your personal data. Only the personal data you choose to enter into our software will be analyzed by the AI. Your personal data will not be used to improve the Machine Learning (ML) analysis.
- Is any data used for machine learning development?
  OpenAI does not use data submitted to and generated by our API to train OpenAI models or improve OpenAI's service offering.
- Does OpenAI train on my content to improve model performance?
  OpenAI will not use data submitted by customers via our API to train or improve our models, unless you explicitly decide to share your data with us for this purpose.
- Where is my AI content stored?
  AI relevant content is stored on OpenAI systems and our trusted service providers' systems in the US and around the world. We may also send select portions of content to third-party contractors (subject to confidentiality and security obligations) for data annotation and safety purposes.
- Do humans view my AI content?
  A limited number of authorized OpenAI personnel, as well as specialized third-party contractors that are subject to confidentiality and security obligations, may view and access user content only as needed for these reasons: (1) investigating abuse or a security incident; (2) to provide support to you if you reach out to us with questions about your account; (3) to comply with legal obligations; or (4) when we fine tune our models using user-submitted data (unless you have opted out), we also use PII filtering techniques to reduce the amount of personal data used. Access to content is subject to technical access controls and limited only to authorized personnel on a need-to-know basis. Additionally, we monitor and log all access to user content and authorized personnel must undergo security and privacy training prior to accessing any user content.
- Is the AI you are using this ChatGPT I read about?
  No. ATLAS.ti is working with OpenAI directly through an interface, and our customers are not using the web interface of the ChatGPT tool. However, the software and model behind the embedded OpenAI software and their ChatGPT tool are similar.
- What is the difference between AI, machine learning, and deep learning?
  AI uses various techniques that allow machines to be artificially intelligent. Machine learning is a subset of AI, and deep learning is a subset of machine learning.
  Machine learning refers to a machine's ability to think without being externally programmed. While devices have traditionally been programmed with a set of rules for how to act, machine learning enables devices to learn directly from the data itself and become more intelligent over time as more data is collected.
  Deep learning is a machine learning technique that uses multiple neural network layers to extract progressively higher-level features from the raw input data. For example, in image processing, lower layers of the neural network may identify edges, while higher layers may identify the concepts relevant to a human, such as letters or faces.

Employees

All ATLAS.ti employees are regularly trained on data protection topics. All employees are obliged to handle personal data confidentially.

Data Portability

Every client can download/export all data processed via ATLAS.ti Web at any time. At the end of the contract, we will ask you to download/export all data and will, after a certain grace period, delete the system and all data.

CCPA

ATLAS.ti does not sell any personal information, we only process our client's data to provide our software and services and we don't use our client's data for any other purposes than to provide our software and services, as described in our Terms & Conditions, our Data Processing Agreement and our Privacy Policy.

Further Questions

For any further questions, please reach out to our data protection officer, Rechtsanwalt Christian Schmoll, at dataprotection@atlasti.com.