AREMIS Trust Center

Information Security

Keeping our customers' information secure is the highest priority at AREMIS. Our security-first approach is fundamental to our business. Our board is committed to providing and maintaining the level of Quality and Information Security that meets all of our stakeholders' needs.

Our purposes are to:

- promote a culture that enables each employee to do their job right, the first time and every time, in a safe and stimulating work environment;
- ensure transparency in our realization of business activities;
- preserve the availability, integrity, confidentiality, and traceability of our information assets and maintain our legal and contractual compliance;
- systematically examine organizational information security risks and implement security controls to address unacceptable risks;
- establish clear and mutually beneficial relationships with relevant interested parties and strive to exceed their expectations where possible.

We incorporate security practices at all levels described in this document.

For this reason, AREMIS has established an Information Security Management System (ISMS) certified ISO27001. This system enables us to systematically operate and maintain information security in our business processes and services, and to determine and apply the necessary security measures based on our risk assessment. We have implemented a security incident management process to detect and remediate security incidents effectively. Regular penetration tests are performed to evaluate our IT infrastructure, identify vulnerabilities, and areas for improvement.

The ISMS allows us to ensure the availability, integrity, confidentiality, and traceability of information.

Security Awareness and Training Practices at AREMIS

One crucial foundation for the effectiveness of the ISMS is the security awareness of all AREMIS employees. AREMIS ensures that its employees stay informed and up-to-date on current issues and best practices in information security through regular training sessions. This includes attending an annual refresher training and completing a test to assess their understanding of our practices and policies.

As part of the induction training, all newly hired employees are required to participate in mandatory information security training. This ensures that they receive the necessary knowledge and awareness from the beginning of their employment. AREMIS employees are expected to adhere to a set of information security policies, which undergo regular reviews to ensure their relevance and effectiveness. Additionally, employees undergo periodic phishing tests to enhance their awareness of cybersecurity threats.

In this section, we provide an overview of the certifications and compliance frameworks that our organization and vendors adheres to. We have undertaken rigorous assessments and implemented robust measures to ensure that our processes, systems, and infrastructure meet the highest standards of security and compliance.

By maintaining these certifications and complying with relevant regulations, we demonstrate our dedication to providing our customers with a secure and trusted environment for their data. We continuously strive to exceed industry standards and evolve our practices to stay ahead of emerging security challenges.

Code of conduct and Confidentiality agreements

AREMIS employees are mandated to sign a code of conduct and a confidentiality clause as an integral part of their employment contract, granting them access to our platform. This clause explicitly prohibits the disclosure of any confidential information pertaining to the business of AREMIS and its customers. These obligations and duties continue to be binding even after the termination of employment.

Certifications

AREMIS' Cloud Services operate under an information security management system that is certified ISO/IEC 27001:2013. This certification signifies adherence to one of the most globally recognized standards for information security in both development and operational aspects.

In addition to being certified ISO/IEC 27001:2013, AREMIS undergoes regular assessments by CyberVadis, a reputable third-party organization specializing in evaluating information security practices. CyberVadis assesses AREMIS' supply chain information security performance and ensures compliance with industry standards. This collaboration highlights AREMIS' commitment to maintaining a robust and secure information security management system, validated by both internal and external assessments.

ISO 27001:2013 CERTIFIED	cybervadis CyberVadis Third Party Risk Management

EU General Data Protection Regulation

In addition to our own compliance, AREMIS is committed to offering services and resources to our customers to help them comply with the GDPR requirements that may apply to their activities.

AREMIS recognizes the significance of the GDPR in enhancing and unifying the protection of personal data belonging to EU citizens. As a data controller, AREMIS is fully committed to adhering to the regulations and implementing industry best practices.

To establish a comprehensive management system, AREMIS utilizes the ISO 27001 standard, for which we hold certification, as a framework. We integrate personal data protection aspects into our management system.

In order to meet the requirements of the GDPR and ensure compliance, we follow the ISO 27701 framework, and our data protection practices undergo third-party audits to verify our adherence to regulations.

We meticulously select our service providers (processors) and require the execution of Data Protection Agreements with them. In cases where data processing occurs outside of the EEA region, we implement either Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCR) to facilitate our operations. We prioritize selecting providers whose subscriptions allow data to be hosted on servers based in Europe.

We use the following major processors:

Processor	Address	Purpose	Trust Center
Microsoft 365	Microsoft Campus, Redmond, WA 98052 USA	Data processing	Additional security information

Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855 Luxembourg	Data Centers used to host AREMIS Cloud Solutions	Additional security information

Reporting GDPR Complaints and Security Breaches: System Overview

AREMIS is committed to protecting the privacy and security of personal data in compliance with the General Data Protection Regulation (GDPR). We have implemented a robust system to report GDPR complaints and security breaches promptly. This section provides an overview of the system and outlines the steps involved in reporting and addressing such incidents.

Reporting Process for GDPR Complaints

a. User reporting:

- To address GDPR-related concerns, AREMIS has established a dedicated process for handling complaints. If you have any GDPR-related complaints or inquiries, we encourage you to reach out to us at gdpr@aremis.com. Our dedicated team will thoroughly review all requests received and ensure they are addressed in accordance with GDPR regulations. We are committed to upholding data protection standards and providing an effective resolution process for GDPR-related matters.

b. Incident Details:

- When reporting a GDPR complaint, users are encouraged to provide specific details, such as the nature of the incident, relevant timestamps, individuals involved, and any supporting evidence.

c. Incident Triage and Assignment:

- Upon receiving a GDPR complaint, the incident is triaged by our dedicated team responsible for data protection and privacy.
- The team evaluates the severity and urgency of the complaint and assigns it to the appropriate personnel for investigation and resolution.

d. Incident Tracking and Communication:

- AREMIS Incident management platform allows for efficient tracking and communication throughout the investigation and resolution process.
- Users can monitor the progress of their complaint and receive updates on the status and resolution steps taken.

Reporting Process for Security Breaches

a. Incident Reporting Channel:

- We maintain a dedicated channel for reporting security breaches, ensuring a prompt and secure means of communication.
- Users can report security breaches through our Incident Management platform or by email via security@aremis.com, which is closely monitored by our security team.

b. Incident Details:

- When reporting a security breach, users are encouraged to provide comprehensive details, including the type of breach, affected systems or data, potential impact, and any relevant evidence or indicators of compromise.

c. Incident Triage and Escalation:

- Our security team promptly triages reported security breaches based on severity, impact, and potential risks.
- Depending on the nature of the breach, the incident may be escalated to higher levels of management or external authorities as required by applicable regulations.

d. Incident Management and Resolution:

- Once a security breach is identified, our security team follows a predefined incident response plan to mitigate the impact, contain the breach, and restore normal operations.
- Communication channels within AREMIS Incident management platform facilitate collaboration, enabling effective incident management and resolution.

Compliance with GDPR and Regulatory Obligations

AREMIS is committed to adhering to ISO/IEC 27001 standards and recognizing the significance of handling requests from country administrative or judiciary authorities. To ensure compliance with legal and regulatory requirements, we have established well-defined procedures in such cases.

Upon receiving a request, we conduct a careful review to assess its legitimacy and scope. Seeking legal counsel, we evaluate the potential implications and risks involved. Throughout this process, we maintain meticulous documentation, recording the request, actions taken, and the legal basis for compliance. Our aim is to strike a balance between fulfilling legal obligations and safeguarding sensitive information, demonstrating our dedication to transparency and privacy protection.

Moreover, we uphold transparency by promptly reporting any disclosures or actions taken to relevant stakeholders, such as data subjects, affected parties, or regulatory bodies, as required by applicable laws and regulations. By upholding these communication protocols, AREMIS exemplifies its commitment to maintaining the highest standards of information security and regulatory compliance.

Additionally, we prioritize thorough documentation and record-keeping practices to ensure compliance with GDPR regulations. This involves maintaining comprehensive records encompassing GDPR complaints, security breaches, incident reports, investigation findings, remediation actions, and communication logs. Such documentation serves as crucial evidence of our compliance with GDPR requirements and facilitates auditing and reporting processes.

In line with our commitment to continuous improvement, we regularly review our incident reporting and response procedures. This ensures their alignment with GDPR guidelines and industry best practices. By actively learning from previous incidents, we integrate valuable insights into our ongoing security and privacy improvement initiatives. This iterative approach ensures that we remain up to date with evolving regulatory requirements and continuously enhance our ability to address potential risks and safeguard the personal data entrusted to us.

Contact with Authorities

Appropriate contacts with legal and regulatory authorities, who oversee information security and privacy, are maintained by our Data Privacy Officer (DPO). These include state, national, and international privacy regulators, in addition to the local authorities.

In the table below we list some of the links to the different agencies or authorities.

Category	Authority	link

GDPR	Belgium - Data Protection Authority	Homepage | Autorité de protection des données Gegevensbeschermingsautoriteit
GDPR	France - CNIL	https://www.cnil.fr/fr/services-en-ligne
GDPR	Switzerland - PFPDT	https://www.edoeb.admin.ch/edoeb/fr/home/actualites/aktuell_news.html
Cyber Security	Centre for Cyber security Belgium	Centre for Cyber security Belgium
Cyber Security	European Cybercrime Centre	Home | Europol