Document version: 2.0
Date of issue: 1.10.2024
Autor: IT Security Team
Approved by: Miroslav Buček, Head of IT Security

Security and compliance

The security of your data is our top priority at Aiviro. We adhere to the highest industry standards to ensure the confidentiality of your data. For Aiviro, processing key business data for companies around the world is part of our daily routine. We are committed to adhering to the highest standards of security and privacy compliance when working with customer data. To this end, we have developed and implemented a comprehensive set of policies, procedures, and controls to ensure the confidentiality, integrity, and availability of your data, as described below.

Security, Legal, and Compliance Department

We have a dedicated security, privacy, and compliance team that manages our security and privacy programs. They design and maintain our defense systems, develop security monitoring processes, and constantly monitor our networks to detect suspicious activity. They also provide expert advice to our technical team. We conduct regular internal audits. In addition, Aiviro appoints a data protection officer and implements data processing, storage, and disposal policies in accordance with the GDPR. If you have any questions about our privacy policy or GDPR compliance, please contact our data protection officer privacy@aiviro.com.

Data protection measures

We adhere to appropriate technical and organizational measures, internal controls, and security routines in accordance with industry best practices. We take technological developments into account to protect your data from accidental loss, destruction, alteration, unauthorized disclosure, or access. These measures include, among other things: ensuring the reliability of employees with access to your data, restricted access, strong authentication, staff training, regular backups, data recovery and incident management procedures, technical protection of the equipment where the data is stored, and more.

Compliance

Aiviro complies with industry standards and regularly checks applications, systems, and networks to ensure continuous protection of your data. We are currently preparing for ISO 27001 certification.

Data processing and transfers

The data collected from you may be transferred, stored, and processed in the European Union. Other options are available as commercial choices. We regularly update our terms and internal data processing procedures to reflect legislative developments and ensure compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and other relevant regulations.

Supplier ecosystem

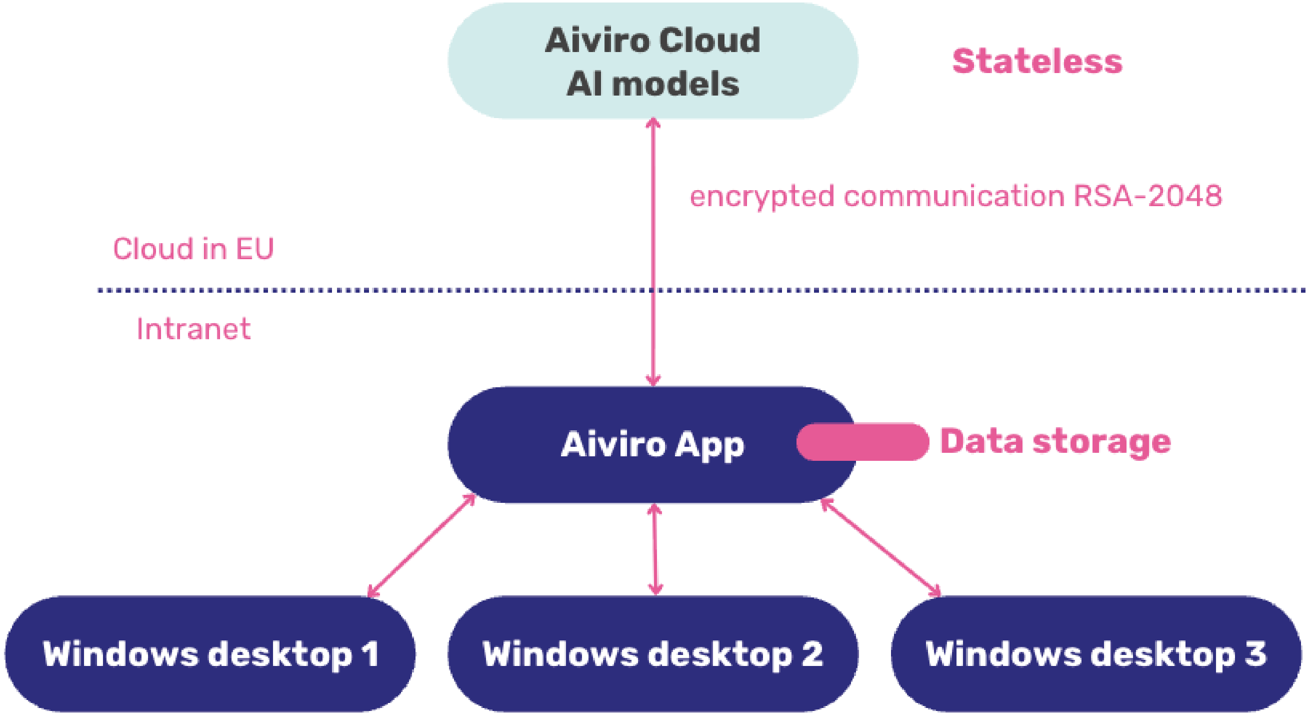
We evaluate each supplier according to our supplier management policy. We accept new suppliers after a thorough risk assessment. We adhere to strict contracts that ensure safety standards and measures.

Data center location

We primarily process data on Google Cloud Platform (GCP) servers, where the main part of our infrastructure runs, which comply with the highest security standards and are regularly audited. At the same time, we use additional services provided by AWS or Azure as needed and according to our customers' specifications. We offer options for different GCP regions according to your data location requirements. European data centers:

- Google GCP: eu-central-1 (Europe – Frankfurt), europe-west1 (certification)
- AWS region: eu-central-1 (Europe – Frankfurt), europe-west1 (certification)
- Azure region: West Europe (Europe – Belgium) (certification)

Our architecture is based on a hybrid model. All data records and their metadata remain with the customer, within their infrastructure. Only the data that is absolutely necessary is sent to the cloud, and only for the time necessary for processing and analysis in the cloud. However, this data is not stored in the cloud; it is only processed and then deleted. All our services run in stateless mode, meaning that no application state is stored between individual requests. Each request is processed as an independent unit that does not require the storage of data about previous operations.



The diagram shows the security architecture of the Aiviro system, which ensures encrypted communication (RSA-2048) between cloud services in the EU (Google OCR, Azure) and internal company resources (Aiviro Manager, log storage, Windows desktops).