Annie Advisor

Security Principles

annieadvisor.com

Table of Contents

Authentication

In order to maintain a secure service, users need to be properly authenticated before being allowed to perform management activities, report faults or request changes to the service.

Identity and authentication

- SAML-based **single sign on** (separately configured for each customer)
  - Azure AD
  - Google SSO
- **Two-factor** authentication
  - Configurable through identity provider

ANNIE RESPONSIBILITY
• Administering user accounts in situations where SSO is not available (e.g. pilot usage)
CUSTOMER RESPONSIBILITY
• Integrating and and managing identity providers for SSO • Onboarding and offboarding users

Access control within Annie

By default, an authenticated user has **no access** to any student data. Access must always be **explicitly granted**. There are different methods for granting access:

- **Relationship-based access**
  - Professionals responsible for certain students are granted access to their students' support requests
  - Access to special support need categories (e.g. mental health) is not included in relationship-based access
- **Category-based access**

    - Support providers are granted access to specific support need categories (e.g. a psychologist gets access to support requests labeled with “mental health”)
- **Privileged access**
    - Annie Admin has access to all support requests within customer’s Annie instance
    - A campaign coordinator has access to all support requests within a support campaign

ANNIE RESPONSIBILITY
• Controlling data access based on customer’s configurations
CUSTOMER RESPONSIBILITY
• Identifying, which support providers should see which support need categories • Providing data on which teachers are responsible for which students • Nominating Annie Admin and campaign coordinator roles

Data security

Data center security

We use UpCloud Ltd as our data center provider. All UpCloud data centres are directly connected to the Internet via transit operators and Internet exchange points (IXPs). Data is **physically located inside the EU area**. Additional requirements regarding data location may be negotiated on a case by case basis.

Data Center Certifications

UpCloud data centres are certified for different requirements such as **ISO9001**, **ISO27001**, **ISO14001**, **ISO14644-8**, **OHSAS 18001**, **PCI DSS**, **PAS 99**, **VAHTI T3** and **KATAKRI**.

2N or N+1 configurations for all critical systems

UpCloud requires all power, cooling and connectivity systems to either have a **stand-in replacement or redundant capacity** in case of breakdowns. This enables the necessary maintenance and handling of unexpected issues without interfering with the infrastructure's operation.

Physical and electronic access control with CCTV monitoring

UpCloud operators control all access to the data centres. There are **physically isolated** sections in the facilities, with **electronic access controls**. Additionally, the whole site is under recorded **video surveillance**.

Onsite 24×7 monitoring of all systems

UpCloud has built their infrastructure with a serious attitude towards high availability to achieve a disruption-free operation. Their internal Operations team **monitors** the cloud environment **around the clock**, working together with the onsite operators.

ANNIE RESPONSIBILITY
• Using secure and trusted data center providers in all operations
CUSTOMER RESPONSIBILITY
• Providing additional requirements regarding data location, if necessary

Data protection

In transit data protection

Encrypted connections (**HTTPS, SSL, TLS, SFTP**, etc.) are always used by default to protect the contents of data in transit.

At rest data protection

All student data including contact information and messaging content is **encrypted at rest** using strong encryption keys and random initialization vectors. Encryption keys are unique for each Annie client instance and stored independently of the database.

ANNIE RESPONSIBILITY
• Encrypting all connections by default • Encrypting personal data at rest
CUSTOMER RESPONSIBILITY
• Using secure channels when transferring data to Annie

Data sanitisation

Data pseudonymization by archiving past campaigns

Support campaigns that are no longer active can be archived. As a part of the archiving process, all personal data except for a pseudonymized identifier is removed. This allows keeping results and insights of past campaigns while removing unnecessary personal data.

Data removal in case of discontinued usage

In the case a client chooses to discontinue using Annie, all data is securely and irreversibly deleted. Before the deletion, the client has an option to get a backup.

ANNIE RESPONSIBILITY
• Providing means to remove or pseudonymize unnecessary data • Securely removing data in case of discontinued usage
CUSTOMER RESPONSIBILITY
• Archiving past campaigns using Annie Admin interface or requesting archiving from Annie personnel

Logging and backups

Logging

Following events are logged

- User logins
- Adding, altering and removing data
- System errors and maintenance events

By default, all logs are stored for two years. Deviation from this can be agreed on a case by case basis. Logs are stored in a widely used format and are transferable to other systems.

Backups

Business continuity is ensured with backups that allow data restore in case of a system failure. By default, daily backups are kept for 7 days, weekly backups for 4 weeks and monthly backups for 12 months. Yearly backups are kept until contract expiration or based on a separate agreement. Recovery tests are carried out at least twice a year.

ANNIE RESPONSIBILITY
• Event logging and log storage • Creating backups and periodically testing backup recovery
CUSTOMER RESPONSIBILITY
• Agreeing on log retention and backup policies

Security Updates

Annie updates customer instances regularly, so that the instances will get the latest security and performance updates.

Critical vulnerabilities

Critical vulnerabilities will be patched without delay.

Non-critical updates

Non-critical updates are installed on the first Monday of every month.

ANNIE RESPONSIBILITY
• Updating customer instances with security updates monthly • Addressing critical vulnerabilities without delay
CUSTOMER RESPONSIBILITY
• Inform Annie of all suspected security issues

Compliance

GDPR

Annie processes personal data only on behalf of the customer (**data controller**). As **a data processor**, we help our customers and users to comply with the General Data Protection Regulation (GDPR). A **data processing agreement** (DPA) is signed with each customer before starting using Annie.

Data location

By default, all data in Annie is **stored inside the EU area** and no data is transferred outside the EU area.

Lawful basis for processing personal data

Basis for data processing **depends on the regulations** applicable in each customer's context. If providing support to students is **a legal obligation** for the customer, GDPR Art. 6 Sec. 1c is applied. Consent of the data subject (GDPR Art. 6 Sec. 1a) is possible but not recommended, if another basis exists.

Categories of personal information

Student **name and phone number are the minimum requirements** of personal information in order to use Annie. Additionally, each customer may choose to include other relevant data regarding their students (educational program etc.), which may then be used in targeting the support campaigns as well as creating support statistics. **Special categories of personal data (GDPR Art. 7 Sec. 1) shall not be included.** Furthermore, we encourage our customers to phrase support categories ambiguously enough not to be interpreted as data concerning health (GDPR Art. 4 Sec. 15).

Data subject rights

GDPR provides data subjects various rights regarding the processing of their data, such as right of access, right to rectification, right to erasure and right to restriction of processing. We **help our customers to answer data subjects' requests** by providing easy ways to access, import and export student and personnel information either inside the Annie Admin interface or as a service. For example, we can provide **a copy of all the personal data being processed about a given data subject** in an electronic format.

ANNIE RESPONSIBILITY
• Acting as a data processor regarding the personal data used in Annie • Providing features and services that help answer requests by data subjects
CUSTOMER RESPONSIBILITY
• Signing Data Processing Agreement (DPA) with Annie

- Acting as a data controller regarding the personal data used in Annie
- Choosing student metadata to include in Annie
- Receiving and processing requests from data subjects

Risk management

We recommend and guide our clients to carry out a data protection impact assessment (DPIA) procedure when starting to use Annie. Impact assessments are designed to identify, evaluate and control risks involved in the processing of personal data. We have gone through this procedure with several clients and can provide templates, information and guidance.

ANNIE RESPONSIBILITY
• Providing templates, information and guidance for impact assessment procedure
CUSTOMER RESPONSIBILITY
• Carrying out impact assessment procedure if necessary