

AFFISE

# Privacy and Data Protection Policies

---

at Affise



ePrivacyse

## 01.

### About Affise

**Affise is a SaaS marketing platform for all types of advertising market players** to grow their business and increase ROI from performance marketing channels. With Affise marketers can easily manage partners and affiliates, discover new partnerships and run the whole ad campaign cycle. Additionally, Affise provides AI-based solutions that allow to automate routine work and make data-driven decisions.

**4**

years  
in the industry

**100+**

professionals  
with over 10 years  
of experience

**1000+**

happy clients

**In 104**

countries  
companies  
use our platform

Nowadays, more and more enterprise businesses are adopting cloud infrastructure on account of lower operating costs, ability to scale, flexibility, and, just as important, data security. **We at Affise seek to protect the data of our customers**, follow the highest standards, and adhere to leading practices in cloud data protection.



## 02.

## Affise Commitment to Data and Security

**We gain the trust and loyalty of our customers** through complete transparency in relationships, accountability, and the way we protect their interests as our own. We care about all aspects of the customer's business, including the legal one. Multi-level data protection systems and strict verification allow us to build long-term relationships with prominent representatives and gurus of the performance marketing industry. As per security responsibilities, shared between Affise and its customers, Affise takes full responsibility for securing the system, thereby enabling customers to focus on business development.

We strictly comply with all the requirements of the relevant organizations by introducing processes and practices for ensuring security and monitoring their implementation. And this document aims to show how mindful we are of this matter and, more crucially, how far we have succeeded in following obligations we have assumed.

### Our Commitments

This white paper provides a list of the technical and operational measures, policies, and practices, applicable as a standard. The measures are designed to:



**Ensure the security** and confidentiality of Personal Data.



**Protect against any anticipated threats** or hazards to the security and integrity of Personal Data.



**Safeguard against any actual unauthorized** processing, loss, use, disclosure, or acquisition of Personal Data.

## 03.

## Affise Security Practices

### People Security

An essential aspect of our data protection framework is the creation and development of a culture of security and privacy awareness. It all starts with the recruiting process: all recruitments follow a screening process according to the Affise background check policy's principles. New employees undergo specialized training, as a part of their onboarding, and are required to agree to security policies, before getting access to the system. All employees take part in mandatory annual training on security and privacy. Affise has implemented various means of internal and external secure communication to ensure the protection of our employees and customers' data.

**To ensure people awareness and compliance with all data updates and procedural processes, Affise takes appropriate measures and continuously conducts necessary training, in particular:**

- All recruitments follow a screening process according to the principles of the Affise background check policy;
- In each contract each employee has Non-Disclosure Agreements clauses;
- Code of Ethics awareness training (including a test) is a yearly obligation for all employees and is to be performed through a dedicated e-learning module;
- Group IT Acceptable Use policy or local version, are shared with all employees;
- Security policy statement signed by the Management is shared with all employees;
- Affise staff is obliged on a yearly basis to follow the Affise Data Protection policy, Information Security and Safety training;

- › Regular awareness training on GDPR for all employees (in addition to Affise Data Protection policy, Information Security and Safety training);
- › Access to systems is provided on a 'need to have basis' taken into account segregation of duties;
- › Regular internal security audits are conducted to verify security practices.

## Product Security

Affise has many years of experience in designing and developing software for the performance marketing industry. This broad expertise makes us aware of the main interaction points where data security must be addressed particularly rigorous



### Encryption

The encrypted connection is enabled to ensure secure delivery and to protect personal data in transit between an Affise client and Affise's system.



### Monitoring and Testing

Affise maintains the best practices in developing secure software. The system undergoes testing before deploying new developments into production. The system also goes through recurring penetration testing once a quarter. In addition to automatic tests, similar manual tests are carried out on a regular basis.



### Access control

Employees with access to private data can only access the data that are necessary for the activities under their responsibility. When Affise's employees interact with customer data, the system logs all activity for security review.

**Following measures related to Access control to Personal Data are in place:**

- The obligation for employees to comply with the applicable Affise group and local security policies and data protection policies;
- Work instructions on handling private data;  
User codes for access to Private Data;
- Differentiated access regulations (e. g. partial blocking);  
Access Logging and control;
- Controlled destruction of data media;
- Procedures for Checking compliance with procedures and work instructions are in place;
- Formalized Control frameworks and TPA to take care that not a single person can access, modify or use critical information assets without authorization or detection.

**Business Continuity and Disaster Recovery** **Disaster recovery**

In the case of natural disasters or system failures, our customers don't have to worry about provisioning and maintenance of software to access real-time information. Affise grants data backup and provides recovery tools to ensure the stable operation of all services.

 **Data deletion**

Affise pledges to delete or return the personal data after termination or expiration of the agreement between Affise and its customers. Deletion is performed in a secure manner, which implies the prevention of illegal access to personal data.

## Security and Confidentiality of Personal Data at Affise

Based on a risk assessment (and if required an additional DPIA) Affise will ensure a level of security appropriate to the risk, including:

- **The anonymization**, pseudonymization (e.g. tokenization) and encryption of Personal Data;
- **The ability to ensure** the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- **The ability to restore** the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- **Ensure a logical separation** between its own data, the data of its customers and suppliers;
- **Set up** a process to keep processed data accurate and reliable;
- **The process registers** according to GDPR requirements;
- **Access** log systems' use with relevant for the purposes of being able to detect unauthorized access attempts;
- **Customer Data** (including back-ups and archives) will only be stored for as long as it serves the purposes for which the data was collected unless there is a legal or contractual obligation to retain the data for a longer period of time.

## 04.

## Affise vs. Customers Relations - Data Controller vs. Data Processor

### Affise as a Data Processor

Affise servers solely as a data processor and has no direct interaction with end-users. Affise values transparency and fulfills obligations towards existing clients, as data-controllers, regarding their requests to delete data containing end user's personal data or any personal data Affise stores regarding its customer's employees, affiliates, and advertisers. Also, Affise pledges to delete or return the personal data after the completion of the processing of personal data (after termination or expiration of the agreement between Affise and its customer) and assist with a data protection impact assessment. Deletion is performed in a secure manner, which implies the prevention of illegal access to personal data.

Affise commits to continuous monitoring the effectiveness of its information safeguards and to a yearly compliance audit by a Third Party to assure the measures and controls in place.

### GDPR Compliance as Shared Responsibility between Data Controllers and Data Processors

#### Data Controller

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**Affise clients are data controllers.**

#### Data Processor

“Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**Affise is a data processor.**

## **Transfer of Data to Customers, Partners or Other Third Parties**

Affise acting as a Data Processor implies that solely under the direction of the customers, Data Controllers, their data can be technically passed on and processed on the Affise platform.

## **Affise as a Supplier of Data Processing**

As a data processor, Affise has no direct interaction with end-users. Affise values transparency and fulfills obligations towards existing clients, as data-controllers, regarding their requests to delete data containing end user's personal data or any personal data Affise stores regarding its customer's employees, affiliates, and advertisers.

## **Data Processing Relations**

Affise stores the data on AWS for the United States and on LeaseWeb Servers for European Union. To meet all legal requirements of the data processing, Affise entered into the data processing agreement with AWS and Leaseweb, which, respectively, meet the legal requirements of art. 28 GDPR.

05.

# Compliance with the Industry Crucial Security Standards



**The ePrivacyseal is a data protection seal of approval following an in-depth audit of a company’s online and mobile products.** The certification covers the requirements of the GDPR for digital products, which catalog of criteria is continuously being adapted to the interpretation of the European and other data protection laws. The ePrivacyseal awards ensure that the company processes the data according to all privacy standards.

**Affise ensures the highest level of security** and meets the certification requirements with state-of-the-art technologies provided by internationally recognized and most comprehensive hosting companies, such as Amazon Web Services and Leaseweb.



**ISO/IEC 27001:2013** is a security management standard that specifies security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidance.



**ISO/IEC 27018:2014** is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO/IEC information security standard 27002 and provides implementation guidance on ISO/IEC 27002 controls applicable to public cloud Personally Identifiable Information (PII).



**SOC 1**  
System and Organization Controls (SOC) is a suite of service offerings CPAs may provide in connection with system-level controls of a service organization or entity-level controls of other organizations.



**California Consumer Privacy Act**  
CCPA is a state-wide data privacy law that regulates how businesses all over the world are allowed to handle the personal information (PI) of California residents.



**ISO 27001**  
The International Organization for Standardization (ISO) 27001:2013 is the international security standard used to benchmark the protection of sensitive data.



**NEN 7510**  
NEN 7510 is the standard developed by the Nederlands Normalisatie Institute for information security in the health sector.

## Conclusion

At Affise we put **Data Security** among the top priorities. With a multi-level data protection system and strict verification implemented in the platform, **Affise delivers a comprehensive solution** that takes care of the legal side of performance marketing and secures the confidentiality of customers' data. We strictly comply with all the requirements of the relevant organizations by introducing processes and practices for ensuring security and monitoring their implementation.

**If you have any questions or seek particular** explanations on topics covered in this you can always contact us through your Customer Success Manager, for clients, or via email.