Security Policy

1. Our policy

At Avent Media, we take the security of your data very seriously. Transparency being one of the core principles of our company, we aim to be as clear and transparent as possible about the way we handle security.
If you have any further questions regarding security, we are happy to answer them. Send an e-mail to gdpr@avent-media.fr and we will respond as quickly as we can.

2. Confidentiality

We place strict controls over our employees' access to the data that you and your users make available through the services deployed by Avent-Media during various campaigns, as more specifically defined in the agreements concluded with our partners covering the use of Avent-Media's services ("Customer Data"). Furthermore, we are committed to ensuring that Customer Data is not seen by anyone who should not have access to it. The operation of Avent-Media's services requires that certain employees have access to the systems which store and process Customer Data. For example, in order to diagnose a problem you are experiencing with Avent-Media's services, we may need to access your Customer Data.
These employees are prohibited from using these permissions to view Customer Data unless it is strictly necessary. We have established technical controls and audit rules (supported by the expertise of Deloitte Consulting) so that any access to Customer Data is logged.
All of our employees and our contract staff are required to comply with our rules regarding Customer Data, and our company treats these issues as matters of the highest priority.

3. Personnel Practices

Avent-Media conducts background checks on all employees before recruitment. Employees regularly receive privacy and security training, including during their first days within the company. All employees are required to read and sign our comprehensive rules regarding information security, which address the security, availability, and confidentiality of Avent-Media's services.

4. Deletion of Customer Data

Avent-Media provides the option for partners to delete Customer Data at any time. Within 24 hours of the deletion by the primary owner, Avent-Media permanently deletes all information from currently-running production systems. Backups of Avent-Media's services are destroyed within 90 days.

5. Encryption of Data Traffic and Storage

Avent-Media's Services support the latest recommended secure cipher suites and protocols to encrypt all traffic. The storage of Customer Data is encrypted.
We closely monitor the changing cryptographic landscape and seek prompt upgrades to respond to emerging threats as they are discovered, and implement best practices as they evolve. Regarding the encryption of data traffic, we do this while attempting to balance the need for compatibility for existing clients.

6. Availability

We understand that you rely on the services we currently provide to run smoothly. We are determined to make our operations a highly-available service that you can count on. Our infrastructure runs on fault-tolerant systems, for individual servers or even entire data centres. Our operations teams regularly test recovery measures after a disaster.

7. Disaster Recovery

Customer Data is stored redundantly at multiple locations in our hosting provider's data centres to ensure availability. Our proven backup and restoration procedures allow recovery from any major disaster. Customer data is automatically backed up every night. This system allows the operations team to be alerted in case of failure. Backups are fully verified at least every 60 days to confirm that our processes and tools work properly.

8. Network Protection

In addition to a sophisticated monitoring of system connections and operation, we have implemented two-factor authentication for all server access across our production environment. Firewalls are configured according to the industry's best practices.

9. Host Management

We perform automated vulnerability scans on our production hosts and address all findings that indicate a risk to our environment. We enforce locking the screens and using full disk encryption for company laptops.

10. Logging

Avent-Media maintains a comprehensive and centralised logging system which contains information concerning security, monitoring, availability, access and other measures relating to Avent-Media's services. These connection logs are analysed for security events via an automated monitoring software under the supervision of the security team.

11. Incident Management and Response

In the event of a system breach/intrusion, Avent-Media will promptly inform you of any unauthorised access to your data. Avent-Media has incident management policies and procedures to handle such eventualities.

12. External Security Audits

We work with respected security firms who perform regular security audits of Avent-Media's services to verify that our security practices are sound, and carry out an analysis of Avent-Media's services to address new vulnerabilities discovered by security research. In addition to periodic and targeted audits of Avent-Media's services and features, we perform a continuous automated verification of our web platforms.

13. Product Security Practices

New features and design changes go through a verification process carried out by the security team. Furthermore, our code is audited with automated statistical analysis software and tested. The security team works closely with the development teams to resolve any security issues that may arise during the development of a campaign or on our platforms.