

Technical and Organisational Measures for AGM@Convene Services

Posting Date: May 2, 2020

Effective date: May 2, 2020

Convene, Azeus and/or its Affiliates (hereinafter “Azeus” and/or “Convene”) have implemented and will maintain appropriate technical and organisational measures for AGM@Convene Services to protect the personal data against misuse and accidental loss or destruction as set forth in this document.

Convene may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

1. Physical Access Control

Unauthorized access (in the physical sense) must be prevented.

Data Centres

- AGM@Convene cloud infrastructure is hosted in Amazon Web Services' (AWS) data centres.
- Physical access to data centres is strictly controlled both at the perimeter and at building ingress points and include, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized data centre staff must pass two-factor authentication a minimum of two times to access data center floors.
- AWS data centres have the following certifications:
 - EU Data Protection
 - AWS generally complies with EU data protection rules.
(<http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/AWS-3-6-15.pdf>)
 - AICPA Service Organization Control Report 3
(https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf)
 - ISO 27001 (https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf)
 - ISO 27017 (https://d0.awsstatic.com/certifications/iso_27017_certification.pdf)
 - ISO 27018 (https://d0.awsstatic.com/certifications/iso_27018_certification.pdf)
 - ISO 9001 (https://d0.awsstatic.com/certifications/iso_9001_certification.pdf)

Convene and/or Azeus Premises

- In general, office buildings or office areas are secured through access control systems. Convene and/or Azeus employees are required to use a fingerprint scan or passcode to access the office buildings or offices and any secure areas.
- Depending on the security classification, individual areas may be further protected by additional measures. These include specific access profiles and video surveillance.
- Guests and visitors to Azeus and/or Convene offices must register their names at reception and must be accompanied by authorized Azeus and/or Convene personnel.
- Administrative access to AGM@Convene cloud infrastructure is limited to the remote access network, i.e. physical access is prohibited.

2. System Access Control

Unauthorized access to IT systems must be prevented.

- AGM@Convene Customers are granted full control on user management in relation to their Events held in AGM@Convene Services. End Users are required to login to be able to access AGM@Convene Services. End Users are identified by their unique usernames.
- Customer's system administrator can define the password policy (e.g. the minimum password length) and sign-in retry limit.
- Administrative access to AGM@Convene cloud infrastructure is limited to the remote access, i.e. physical access is prohibited.
- Authorized personnel are provided individual accounts for proper access control and auditing. User access review is performed on a regular basis. All access to the AGM@Convene cloud infrastructure requires strong authentication.
- AGM@Convene cloud infrastructure has a 24x7 intrusion detection system.
- The company network is protected from the public network by firewalls.
- Security patch management is implemented to ensure regular deployment of relevant security updates.
- Full remote access to Convene/Azeus' corporate network and critical infrastructure is prohibited. Special approval from senior management is required and such access is protected by strong authentication.

3. Data Access Control

Activities in IT systems not covered by the allocated access rights must be prevented.

- AGM@Convene Customers are granted full control on access management in relation to their Events held in AGM@Convene Services. End Users are required to login to be able to access data in AGM@Convene Services. Only authorized End Users with appropriate permission can access the data. No Convene/Azeus employee will have access to or will be able to view data submitted or uploaded by End Users to AGM@Convene servers for the Events, unless authorised by you for the purpose of delivering the Services.
- Authorisation mechanisms have been implemented within AGM@Convene Services to enable Customers to manage and authorize access of data by their End Users.
- Audit trail has been implemented within AGM@Convene Services to allow Customer's system administrator to review their End User access logs when necessary.

4. Data Access Control

Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.

- AGM@Convene Customers are granted with full control on data management and content of the data uploaded or submitted to AGM@Convene in relation to their Events held in AGM@Convene Services.
- Only authorized End Users with appropriate permission can access and transmit the data.

5. Data Access Control

Full records (such as logging system) of data management and maintenance must be maintained.

- All servers within the AGM@Convene cloud infrastructure are protected via different measures including hardening based on industry security benchmarks and 24x7 intrusion detection system to ensure no unauthorized data input to the system.
- AGM@Convene Customers are granted full control on access management in relation to their Events held in AGM@Convene Services. End Users are required to login to be able to access and input data in AGM@Convene Services.
- Audit trail has been implemented within Convene Services to allow Customer's system administrator to review their End User access logs when necessary

6. Job control

Commissioned data processing must be carried out according to instructions.

- Personal Data being processed on commission (i.e. Personal Data processed on a Customer's behalf in relation to Events) is processed solely in accordance with the relevant agreement and related instructions of the Customer.
- Convene Customers are granted full control on data submitted or uploaded to Convene in relation to their Events held in AGM@Convene Services. No Azeus and/or Convene employee will have access to or will be able to view data submitted or uploaded by End Users to AGM@Convene servers for the Events, unless authorised by you for the purpose of delivering the Services.
- All Azeus and/or Convene employees and contractual sub-processors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Azeus and/or Convene customers and partners.

7. Availability control

The data must be protected against accidental destruction or loss.

- AGM@Convene cloud infrastructure is hosted in AWS data centres which guarantees high reliability and availability.
- The AGM@Convene system is configured to perform regular automated backups. Recovery point objective (RPO) and recovery time objective (RTO) for disaster recovery situations are defined.
- Convene employs backup processes and other measures that ensure rapid restoration of business-critical systems as and when necessary.
- Convene has defined contingency plans as well as business and disaster recovery strategies for the provided Services.

8. Data Segregation Control

Data collected for different purposes must also be processed separately.

- The AGM@Convene cloud infrastructure is hosted in AWS data centres. Each Customer has its own single-tenanted environment to ensure that data is separated from other Customers.
- All AGM@Convene servers are hosted within a Virtual Private Cloud (VPC) that logically separates the AGM@Convene cloud infrastructure with other tenants within the public cloud.