Technical and Organisational Measures

Published on: 13 October 2022

Azeus and/or its Affiliates have implemented and will maintain appropriate technical and organisational measures for Convene ESG Services to protect the personal data against misuse and accidental loss or destruction as set forth in this document.

Azeus 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

- Convene ESG cloud infrastructure is hosted in highly secure and reliable data centres including 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:
  - GDPR compliance (https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/)
  - AICPA Service Organization Control Report 3 (https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.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)

Azeus Premises

- In general, office buildings or office areas are secured through access control systems. 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 offices must register their names at reception and must be accompanied by authorized Azeus personnel.
- Administrative access to Convene ESG 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.

- Convene ESG Customers are granted full control on user management. End Users are required to login to be able to access Convene ESG Services. End Users are identified by their unique user names. All documents uploaded by End Users to Convene ESG Services are encrypted using AES-256.
- Administrative access to Convene ESG 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 Convene ESG cloud infrastructure requires strong authentication.
- Convene ESG 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 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.

- Convene ESG Customers are granted full control on access management. End Users are required to login to be able to access data uploaded to Convene ESG Services. Only authorized End Users with appropriate permission can access the data. Azeus do not directly access customer data except as authorized by End Users or as necessary to provide services to the Customer such as permitting its ESG Experts to have access to the data relevant to ESG reportorial requirements for the sole purpose of assisting the Customer in achieving compliance of ESG sustainability reports as required by the authorities.
- Authorisation mechanisms have been implemented within Convene ESG Services to enable Customers to manage and authorize access of data by their End Users.
- Audit trail has been implemented within Convene ESG Services to allow Customer's system administrator to review End User access logs when necessary.

4. Data Transmission Control

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

- Convene ESG Customers are granted with full control on data management and content of the documents uploaded in Convene ESG
- Only authorized End Users with appropriate permission can access and transmit the data.
- All documents uploaded to Convene ESG are encrypted both during storage and in-transit.

5. Data Input control

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

- All servers within the Convene ESG 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.
- Convene ESG Customers are granted full control on access management. End Users are required to login to be able to access and input data in Convene ESG Services.
- Audit trail has been implemented within Convene ESG Services to allow Customer's system administrator to review 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) is processed solely in accordance with the relevant agreement and related instructions of the Customer.
- Convene ESG Customers are granted full control on data uploaded to Convene ESG. No Azeus employee will have access to or will be able to view data uploaded by End Users to Convene ESG servers.
- All Azeus 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 customers and partners.

7. Availability control

The data must be protected against accidental destruction or loss.

- Convene ESG cloud infrastructure is hosted in highly secure and reliable data centres which guarantees high reliability and availability.
- The Convene ESG system is configured to perform regular automated backups. Recovery point objective (RPO) and recovery time objective (RTO) for disaster recovery situations are defined.
- Azeus employs backup processes and other measures that ensure rapid restoration of business-critical systems as and when necessary.

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