OrgVue

SECURITY

GDPR Compliance Overview

This document is intended to provide information and assurance on the key security and data protection controls for OrgVue. OrgVue supports compliance with international data protection legislation through a combination of logical controls built-in to the application and those which Concentra adopts as an organisation.

This document supports our Data Processing Provisions and Security Provisions which can be found at: http://www.concentra.co.uk/terms-and-conditions

As an ISO 27001:2013 and CSA STAR certified organisation, Concentra is fully committed to information security for OrgVue by providing resource and financial commitments to the establishment, adoption and continual improvement of our security controls and procedures. Security is built-in to the development lifecycle of OrgVue with risks being continually assessed as part of development and quality control processes.

OrgVue is delivered as Software as a Service, developed internally by Concentra and hosted on the Amazon Web Services (AWS) platform.

With reference to the GDPR and broader international data protection legislation, as an OrgVue client you are the **Data Controller** for personal data which you upload into OrgVue and Concentra Consulting Ltd is the **Data Processor**. Our legal basis for processing any personal data you upload into your OrgVue tenant will always be founded on the performance of the contract we have with you.

As a Data Processor, Concentra delivers compliance with its GDPR obligations to provide sufficient guarantees in implementing appropriate technical and organisational measures, notably through our ISO 27001:2013 and CSA STAR certifications. These are supported by the extensive security and data protection controls we have in place for the OrgVue application which we describe in detail in our product security documentation. This documentation also includes the security measures built into the Amazon Web Services (AWS) platform which OrgVue is hosted from and information on how we approach security as an organisation.

OrgVue has always held the principle of '**Data protection by design and by default**' as a core pillar of its architecture and security posture. As a true multi-tenanted environment, each OrgVue client tenant is logically separated and uniquely encrypted using a dedicated encryption key, ensuring appropriate technical measures are in place to safeguard your data. This is augmented by our access security model which means that you have exclusive control over access to your OrgVue data, while Concentra has no access unless you authorise and engage us to.

To ensure the ongoing confidentiality, integrity, availability and resilience of OrgVue data processing, our adoption of the Amazon Web Services (AWS) platform for OrgVue hosting has enabled us to provide industry leading levels of security, resiliency and scalability which we deliver to you. More information on AWS compliance programs is available at https://aws.amazon.com/compliance/programs/

The terms of the OrgVue licence includes our commitment to you that we will notify you of any intended changes concerning the addition or replacement of processors. Apart from Concentra, only AWS is involved in the delivery of the OrgVue service and has no access to your OrgVue data.

Currently we offer two global regions for you to host your OrgVue data from, one in the US and one in the EU, with future support for more locations planned. Once you have selected a region, your data will remain in that region only and would not be transferred out of that region without your prior written consent.

In selecting AWS we have chosen a hosting provider whose own Data Processing Addendum includes EU Model Clauses, which have been approved by the EU Article 29 Working Party. More information is available here: https://aws.amazon.com/compliance/eu-data-protection/

Our Data Protection Schedule also includes our commitment to you that we will retain your OrgVue tenant data for up to 90 days at the end of your relationship with us, or shorter if you require. At which point your data will be destroyed and rendered unrecoverable.

The following sections provide further detail on the information security and data protection controls we implement to safeguard your data:

Organisation of Information Security

Concentra's commitment to data security and privacy is reflected at all levels throughout the organisation. Concentra has a dedicated Information Security team and Data Protection Officer, with governance in place through an Information Governance Board led by C-Level Executives. An established risk management program is in place with Board level visibility.

Human Resource Security

All Concentra staff are subject to criminal record checks as part of our standard screening process for new employees, which includes extensive background verification of previous employment and educational certificates.

Formal Information Security and Data Protection training is mandatory for all staff and delivered through an online LMS platform. Awareness training is complemented through company presentations, newsletters and induction sessions.

Asset Management

Within our organisation, owners of physical and information assets are recorded with clear responsibilities outlined. These responsibilities include management of access to information assets, assignment of information classifications and retention periods.

Access Control

A key security principle of OrgVue is the client's exclusive control over access to the application and the data within. Authentication via Single Sign-On (SSO) is strongly recommended, enabling a client's own internal access control policies to be extended to their OrgVue environment. Authentication via SSO enables support for Multi-Factor Authentication.

OrgVue supports both role-based and attribute-based access control, providing very fine levels of granular access control when required.

From an organisational perspective, Concentra access control changes relating to role moves and departures from the organisation are closely managed, with all access to Concentra's own internal systems removed on date of departure. The principles of least privilege and need to know are embedded in the organisation's access control methodology.

Encryption

Encryption is at the core of OrgVue's information security and data protection controls.

Each OrgVue client tenant is uniquely encrypted via AES-256 (GCM) with a dedicated encryption key. AES remains the global benchmark for symmetric encryption at rest. OrgVue encrypts all data at rest through the application itself. As the data is encrypted through the application, the encrypted state persists through into the backup media, which also remains within the same AWS geographical region as production data.

All OrgVue data in transit is encrypted via HTTPS over TLS 1.2 with 256-bit encryption.

In order to manage access to OrgVue tenant encryption keys, OrgVue uses the AWS Key Management Service (KMS) which is an automated service meeting the US Federal FIPS-140 standard.

Physical and Environment Security

OrgVue is hosted at Amazon Web Services (AWS) data centre facilities providing benchmark levels of physical and environmental security controls. Information on AWS compliance programs is available at: https://aws.amazon.com/compliance/programs/

In the interests of security, AWS do not publish physical address details for their data centre locations.

From an organisational perspective, Concentra offices are managed with extensive physical security controls and have been independently audited for compliance with the requirements of the ISO 27001 standard.

The following sections provide further detail on the information security and data protection controls we implement to safeguard your data:

Operational Security

OrgVue servers are protected by full endpoint protection services, incorporating Anti-Virus, Intrusion Protection and Data Loss Prevention controls. The AWS environment provides additional controls, notably in the form of AWS Shield for managed DDoS protection and the AWS GuardDuty service which delivers intelligent threat detection and continuous monitoring.

OrgVue backups are made on a nightly basis and retained for 30 days.

Communications Security

All OrgVue data in transit is encrypted via HTTPS over TLS 1.2 with 256-bit encryption. Data transfers are uploaded directly in to the encrypted tenant environment. OrgVue provides full support for data extract with common file types such as CSV supported, enabling extraction and data porting in standard forms.

Systems Acquisition Development and Maintenance

Concentra manages all OrgVue code development internally. This approach enables consistent levels of information security throughout an established SDLC process, while remaining agile in providing rapid updates and feature improvements through a DevOps and Continuous Delivery framework.

All Developers receive training in secure coding practices which are aligned to the OWASP Top 10 Application Security Risks.

Supplier Relationships

Concentra directly manages the delivery of all OrgVue services with Amazon Web Services (AWS) being the only third party involved. AWS have no access to OrgVue data. Any change to existing or the introduction of new processors to the OrgVue service would be communicated to and approved by our clients.

Information Security Incident Management

Concentra has an established Incident Management process incorporating root cause analysis and corrective action remediation. Incident Managers have direct access to Executive leadership to ensure all appropriate resources are available. Any incident impacting the information security or privacy of OrgVue data would be reported to our clients within 24 hours of discovery, which is formalized through the OrgVue Security Provisions.

Business Continuity

OrgVue leverages multiple Availability Zones within the AWS infrastructure, providing very high levels of fault tolerance and resiliency. AWS Availability Zones enable OrgVue to be supported from multiple diverse locations, providing continuous service levels, while retaining data within the same geographical region.

From an organisational perspective, Concentra has an established business continuity planning strategy and takes a cloud-first approach to its own internal systems, reducing dependency on physical infrastructure and office locations.

Compliance, Security Certifications and Audits

Concentra is ISO 27001:2013 and CSA (Cloud Security Alliance) STAR certified. Ongoing compliance with these standards ensures that Concentra's information security management system is routinely reviewed and audited by external independent bodies.

In addition, Concentra completes two web application penetration tests per year for OrgVue, which contribute to the continual improvement of the security posture of OrgVue.