DataPlus

By CONCENTRA

SECURITY

This statement is intended to provide information and assurance on how DataPlus has been designed to segregate and protect customer data and how Concentra meets key Information Security requirements from an organisational perspective.

This document supports the Concentra Data Protection Schedules and the DataPlus Security Schedule.

As a DataPlus client you are the **Data Controller** for data you upload into DataPlus and Concentra Consulting Ltd is the **Data Processor**. Our legal basis for processing any data you upload into your DataPlus tenant will always be founded on the performance of the contract we have with you.

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

DataPlus has always held the principle of **'Secure by Design'** as a core pillar of its architecture and security posture. As a true multi-tenanted environment, each DataPlus client tenant is logically separated, ensuring appropriate technical measures are in place to safeguard your data.

To meet requirements related to the ongoing confidentiality, integrity, availability and resilience of our processing, our adoption of the Azure platform for DataPlus hosting has enabled us to provide industry leading levels of security, resiliency and scalability which we deliver to you. More information on Azure compliance programs is available at **https://azure.microsoft.com/en-gb/overview/trusted-cloud/**

The terms of the DataPlus 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 Microsoft (via the Azure platform) is involved in the delivery of the DataPlus service and has no access to your data on DataPlus.

Currently we offer DataPlus in the EU region only, with future support for more locations planned. Your data will remain in the deployed region only and will not be transferred to any other region as they become available without prior agreement.

In selecting Azure we have chosen a hosting provider who complies with EU Model Clauses and whose platform enables ISVs to maintain compliance with the requirements of GDPR. More information is available here: **https://www.microsoft.com/en-us/trustcenter/Privacy/GDPR**

Our Security Schedule also includes our commitment to you that we will retain your DataPlus tenant data for up to 10 working days at the end of your relationship with us, or shorter if you require. At which point your data will be destroyed and ultimately rendered unrecoverable after our 30 day backup retention cycle has passed.

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 for 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 DataPlus is the client's control over access to the application and the data within. Authentication is via Single Sign-On (SSO) only, enabling a client's own internal access control policies to be extended to their DataPlus environment. Authentication via SSO enables support for Multi-Factor Authentication.

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 DataPlus' information security and data protection controls.

Each DataPlus client tenant is encrypted via AES-256 (GCM). AES remains the global benchmark for symmetric encryption at rest. DataPlus encrypts all data at rest using default encryption in place on the Azure platform.

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

Physical and Environment Security

DataPlus is hosted in Microsoft Azure data centre facilities providing benchmark levels of physical and environmental security controls. Information on Azure compliance programs is available at: **https://azure.microsoft.com/en-gb/overview/trusted-cloud/**

In the interests of security, Microsoft do not publish physical address details for their Azure 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.

Operational Security

DataPlus utilised serverless technologies on the Azure platform which are protected by full endpoint protection services, incorporating Anti-Virus, Intrusion Protection and Data Loss Prevention controls. The Azure environment provides additional controls, notably in the form of Azure Security Centre and Advanced Threat Protection delivering intelligent threat detection and continuous monitoring.

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

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

Communications Security

All DataPlus data in transit is encrypted via HTTPS over TLS 1.2 with 256-bit encryption. Data transfers are uploaded directly in to the segregated tenant environment.

Systems Acquisition Development and Maintenance

Concentra manages all DataPlus 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 DataPlus services with Microsoft Azure being the only third party involved. Microsoft Azure has no open access to DataPlus data. Any change to existing or the introduction of new processors to the DataPlus 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 your DataPlus data would be reported to our clients within 24 hours of discovery, which is formalized through the DataPlus Security Schedule.

Business Continuity

DataPlus leverages multiple Availability Zones within with the Azure infrastructure providing very high levels of fault tolerance and resiliency. Azure Availability Zones enable DataPlus 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 DataPlus, which contribute to the continual improvement of the security posture of DataPlus.