General Security Documentation

Flex Applications utilizes Microsoft Azure as the cloud hosting platform. Azure provides a secure, scalable, and compliant environment for application hosting and data storage.

Azure complies with multiple international security standards, including:

- ISO 27001
- SOC 1, SOC 2, SOC 3
- GDPR (General Data Protection Regulation)

Flex Applications has an internal security governance structure with clear roles and responsibilities, ensuring ongoing evaluation and enhancement of security measures.

1. Data Protection and GDPR Compliance

Data Location: All customer data is stored within Microsoft's **European datacenters**, ensuring GDPR compliance.

Data Encryption:

- Data is encrypted both **at rest** and **in transit** using industry standards such as **AES-256** and **TLS 1.2/1.3**.
- Encryption keys are securely managed following Azure Key Vault best practices.

Backup and Data Recovery:

- Regular, automated backups are performed.
- Point in Time Restore: 14 days.
- Differential backup frequency: 12 hours.
- Long-term retention: 1 month.
- Disaster recovery plans are in place to minimize downtime and data loss.

Data Subject Rights: Flex Applications ensures customer rights under GDPR, including the right to data access, correction, portability, and deletion.

2. Access Management

Access Control:

- Role-Based Access Control (RBAC) is implemented to ensure users have appropriate access based on their responsibilities. Implementation of Time-Based Access Control is in progress.
- Access rights are reviewed periodically.

Authentication Methods:

- Visma Connect offers modern authentication methods, including **Multi-Factor Authentication (MFA)** such as BankID, Face ID, and Touch ID.

Audit and Monitoring:

- Access to systems and data is logged and monitored continuously.
- Regular audits are conducted to ensure compliance with access policies.

3. Incident Management

Incident Detection and Response:

- Flex Applications maintains a formal **Incident Response Plan**.
- Incidents are promptly identified, contained, investigated, and resolved.

Customer Notification:

- In the event of a data breach or incident affecting customer data, customers are notified in accordance with GDPR requirements.

4. Subprocessors and Third-Party Providers

Use of Subprocessors:

- Flex Applications primarily relies on **Microsoft Azure** as its cloud service provider.
- All subprocessors are evaluated for their security and compliance posture.

Data Processing Agreements (DPA):

- DPAs are in place with all relevant subprocessors.
- A maintained list of subprocessors is available here.

5. Vulnerability Management and Patch Management

Security Updates:

- Security patches for the application and underlying infrastructure are applied promptly according to a structured vulnerability management process.

Vulnerability Scanning and Remediation:

- Regular vulnerability scans are conducted.
- Identified vulnerabilities are assessed and prioritized for remediation based on risk severity.

Summary

Flex Applications' transition to Microsoft Azure, together with the implementation of Visma Connect for secure authentication, ensures a high level of data security, GDPR compliance, and operational resilience. Comprehensive measures are in place to protect customer data, manage risks proactively, and support customer compliance needs.

For further questions, please contact oskar.anderstal@flexapplications.se

---

This document is intended to assist customers and their IT departments during cloud security reviews related to Flex Applications' migration to Azure and Visma Connect.