Go1 – Technical and Organizational Measures (TOMs)

The technical and organizational measures (TOMs) provided below have been implemented for the Go1 platform in the production environment.

Confidentiality of processing systems

Security Framework

- Go1 has implemented its Information Security Management System in line with the requirements outlined in ISO 27001:2013.

Identity and Access Management

- Administrator access to Go1 production systems is granted based on job roles and responsibilities and is limited to authorized personnel.
- Access to personal data stored in Go1 production systems (servers, applications, databases) is only provided to employees with clear business needs and in line with their job role and responsibilities.

Audit Assurance: Compliance, Governance and Risk Management

- Go1 performs vendor security reviews for third-party vendors whose services will store, process or transmit Go1 and/or Go1 customer data.
- Go1 performs regular risk assessments of production applications and services. Results from these risk assessments are documented in a risk register and prioritized for treatment based on risk level.

Human resources

- Go1 team members complete security awareness training upon hire and annually thereafter.
- To the extent legally permissible, a background check is performed on Go1 new hires as a condition of employment.

Integrity of processing systems

Application & Infrastructure Security

- Infrastructure management and configuration management tools are used for security hardening and to ensure baseline configuration standards have been established for production systems.
- Monitoring tools are used to continuously monitor security events, application performance, network performance and cloud service performance.

- An issue tracking system is in place to centrally record, manage, and monitor application and infrastructure changes from development through to production.

Threat and Vulnerability Management

- Go1 conducts third-party application penetration testing on a bi-annual basis.
- Go1 maintains an incident response plan and follows documented incident response policies including data breach notification in the event of a known or suspected breach of customer personal data.

Availability of processing systems

- Go1 has a business continuity plan in place and performs business continuity and disaster recovery tabletop exercises on an annual basis.
- Monitoring tools are used to monitor in scope systems and alert the relevant teams before capacity thresholds are met.

Additional Considerations

- Microsoft Azure and AWS are responsible for implementing controls to manage physical and logical access to the servers and supporting infrastructure, and underlying network and virtualization management software for its cloud hosting services where Go1 processing systems reside. Go1 processing systems do not reside in any of the Go1 offices.

This TOMs was updated and effective as of November 2023