Technical and Organizational Measures

Qrator Labs CZ s.r.o. (the Czech Republic) and their subsidiaries and affiliated companies (together, “Qrator”, “we”, “us” or “our”) are committed maintaining your privacy and implemented the following measures.

INFRASTRUCTURE SECURITY

Qrator hosts data at trusted geographically-distributed data centers within European Union locations.

The data centers employ the highest standards of physical security to restrict unauthorized physical access and protect the safety of customer data. Only authorized personnel have access to the data centers, based on strict access management, control protocols, and monitoring by surveillance cameras (CCTV).

The data centers’ electrical power systems are designed to provide uninterrupted power supply to the entire infrastructure 24 hours a day, 7 days a week. The data centers are powered by at least two independent power sources. The use of automatic uninterruptible power supplies protects against power surges in case of switching power lines and provides power support during the switchover to diesel generators.

High-availability and redundant infrastructure are designed to minimize associated risks and eliminate single points of failure.

This redundant infrastructure allows Qrator to fulfill most types of preventives and maintenance. Scheduled maintenance and change to the infrastructure are carried out in accordance with the manufacturers’ specifications and internal documented procedures.

For all critical data, Qrator maintains business continuity and disaster recovery plans that are periodically tested. Recovery point and time objectives for processed data are established according to criticality of their characteristics.

Qrator provides real-time encryption for all data transferred among customers and data centers, among Qrator employees and data centers and among the data centers. This real-time encryption provides the best protection for network interaction and prevents unauthorized access (reading, changing or deleting or making copies) to the transmitted data.

Qrator network is multi-layered and zone-based. The managed network equipment separates and isolates internal, external and customers’ environments, and provides routing and filtering of network protocols and packets.

ACCESS CONTROL

Qrator has implemented an enterprise-wide access control policy to restrict access to information resources and data in accordance with official duties. Access provisioning is based on the «Need to Know» and «Least Privileges» principles.

Internal access control procedures detect and prevent unauthorized access to Qrator systems and information resources. When providing access, Qrator uses centralized access control systems with secure mechanisms and authentication protocols, unique user IDs, strong passwords, two-factor authentication mechanisms and limited control access lists to minimize the likelihood of unauthorized access.

In addition, any access is recorded in system audit logs, changes to which are not allowed. The audit logs are periodically reviewed.

DATA STORAGE SECURITY

The architecture of Qrator data storage provides physical and logical isolation and separation of data to ensure processing of the minimum amount of data in accordance with the stated processing purposes.

The disks and equipment on which the data storage and / or processing are carried out can be broken, switched out for repair or decommissioned. In these cases, Qrator takes measures aimed at a complete erasure of data from disks and the removal of residual data from the internal memory of the equipment. In the event that it is not possible to erase (delete) such information, physical destruction of equipment is performed in a way that makes it impossible to read (restore) such data.

PERSONNEL SECURITY

Its personnel are Qrator most important asset. Personnel are obligated to comply with Qrator' confidentiality, business ethics and code of conduct policies. Qrator pays special attention to the selection of personnel by conducting appropriate background verification checks on candidates for employment in accordance with applicable local laws, statutory regulations and ethics.

All employees receive awareness education and training regarding information security, privacy protection and data processing, as is appropriate relative to their job functions and assigned roles.

SUPPLIER RELATIONSHIP

Before contracting with any third-party subprocessor or service provider, Qrator conducts a thorough diligence process to ensure each third party can provide an appropriate level of security and privacy corresponding to the level of data access. Contracts with third parties contain privacy and confidentiality requirements.