

Technical & Organizational Measures for Information Security & Data Protection

Raptor Customer Data Platform
Version: 1.0

The level of security shall take into account:

That the processing involves a varying volume of personal data which are not subject to Article 9 GDPR on 'special categories of personal data' which is why a 'low' level of security should be established.

The Processor shall hereafter be entitled and under obligation to make decisions about the technical and organizational security measures that are to be applied to create the necessary (and agreed) level of data security.

The Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Controller:

- Requirements for pseudonymization and encryption of personal data
- Personal data is encrypted at-rest and in-transit according to best practice. Occasionally, copies of personal data are decrypted in local secure environments, after which the data is deleted. Transfers between environments are encrypted, and local devices store data on encrypted hard drives.

Requirements for ensuring ongoing confidentiality, integrity, availability and robustness of processing systems and services:

- Firewall
- Antivirus
- Protection against DDoS attacks
- Logging
- Access control
- User management
 - Account closure and access upon termination by the data controller
- Vulnerability scanning and penetration testing
- Patching
- Network segmentation
- MFA
- Physical security in offices
- Encryption
- Personnel security when hiring and terminating
- IT security policy
- Data processing policy and procedures
- Awareness and training
- Management of and requirements for sub-processors
- Contingency plan
- Documentation of systems, processes, treatments, etc.
- Regular checking and re-evaluation of security measures
- Security during sending and transferring data sets as well as deleting local copies
- Control of deletion incl. random samples

Requirements for the ability to promptly restore the availability of and access to personal information in the event of a physical or technical incident:

- All systems are monitored 24 hours a day by an operations supervisor who can immediately respond to operational problems
- The majority of the systems have built-in redundancy
- In the event of a disaster scenario, the system will be able to be restored using backups within approx. 12 hours.

Requirements regarding procedures for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing safety:

- Regular checks of data processing procedures and policies
- Self-check according to ISAE 3000
- Annual ISAE 3000 audit by external auditors
- Regular risk assessment of treatment safety
- Ongoing monitoring of legislation and changes to it
- Audits of sub-processors

Requirements regarding access to the information via the Internet:

- All data and information about the registered can be accessed via the Provider system's internet-based user interface.
- Access rights to information are managed by an administrator appointed by the Customer.
 - It is therefore only the Customer who decides which parts of the system's functions and data the individual user has access to.
 - This applies to all users of the system, both internal employees and external users, including the Provider employees.

Requirements regarding the protection of information during transmission:

- HTTPS and TLS 1.2 certificate at API and application level
- Security during sending and transferring data sets as well as deleting local copies
- Control of deletion incl. random samples
- Requirements regarding the protection of information during storage:
- Access control
- Logging
- Monitoring
- Encryption at infrastructure level (at-rest) with encryption algorithm 256-bit AES
- Backup

Requirements regarding physical security of locations where information is processed:

- All data is stored with Microsoft Azure and is therefore subject to their standards for physical access to their hosting centers
- Physical locations are secured with key access and secured against intruders outside opening hours

Requirements regarding the use of home/remote workplaces:

- All remote work is subject to the same guidelines as when working at the company's locations
- Awareness – Employees are continuously trained to avoid the risks associated with remote work
- Critical infrastructure is accessed via VPN
- IP whitelisting for critical infrastructure

Requirements regarding logging:

- Logging of data processing systems and access to services that process data, including:
 - Access logs
 - Event logs
 - API logs
 - Error log
 - Security log
 - Application logs

All logs are configured and reviewed by relevant staff.

Procedures for the Controller's audits, including inspections, of the processing of personal data being performed by the Processor

The Processor shall annually at the Processor's expense obtain an auditor's report from an independent third party concerning the Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions.

The Provider undergoes an annual ISAE 3000 Type II audit conducted by an external state-authorized and certified public accountant.

The Parties have agreed that the following types of auditor's report may be used in compliance with the Contract:

- ISAE 3000

The auditor's report shall without undue delay be submitted to the Controller for information. The Controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Contract.

The Controller or the Controller's representative shall in addition have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the Processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the Controller deems it required.

Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The Processor shall annually at the Processor's expense obtain an auditor's report/inspection report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Contract.

The parties have agreed that the following types of auditor's report/inspection report may be used:

- ISAE 3000 (FSR/Datatilsynet)
- ISAE 3000 / SOC II
- ISO 27001 + ISO 27018
- ISO 27701
- EU Cloud Code of Conduct

- CSA Code of Conduct for GDPR Compliance
- BS 10012

The auditor's report/inspection report shall without undue delay be submitted to the data controller for information. The Controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the Controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Contract.

The Processor or the Processor's representative shall in addition have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the Processor (or the data controller) deems it required.

Documentation for such inspections shall without delay be submitted to the Controller for information. The Controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.