Technical and Organizational Measures (TOMs) pursuant to Art. 28 DSGVO, as of 14.08.2023

This chapter describes the technical and organizational measures implemented by oculavis SHARE Software, oculavis SHARE Apps and the development company oculavis GmbH. These measures are binding and apply to all cases of data processing activities. The implemented measures take into account the state of the art according to guidelines/policies of the Federal Office for Information Security (BSI) and the recommendations of the IT Security Association Germany. The data protection officer of oculavis GmbH assures the fulfilment of TOM and guarantees in the long run that the selected technical and organizational measures for the present data processing by oculavis GmbH will remain in force.

ID	Measure	Description
1. Certifications		
1.1	Certifications	oculavis is ISO 27001 furthermore oculavis' hosting providers have several certifications, see also: - Microsoft: https://azure.microsoft.com/de-de/explore/trusted-cloud/compliance/ - T-Systems: https://www.open-telekom-cloud.com/en/products-services/core-services/certifications
1.2	Hosting Providers	We currently support the following hosting providers with the appropriate technical and organizational security measures: - Microsoft: https://azure.microsoft.com/en-gb/explore/trusted-cloud/compliance/ - T-Systems: https://www.telekom.com/de/konzern/datenschutz-und-sicherheit/news/privacy-and-security-assessment-verfahren-342724
2. Audit & Assurance		
2.1	Audit and Assurance Policy and Procedures	Internal privacy and IT security policies (based on the ISMS ISO 27001 Norm), including procedures under applicable laws and regulations, are implemented and regularly (in general on an annual basis) reviewed and updated, as necessary.
2.2	Independent Assessments	Based on ISO 27001 requirements, our policies and regulations are audited by an external auditor on an annual basis.
2.3	Risk Based Planning Assessment	Based on risk management, internal systems and their responsible parties are additionally monitored and audited.
2.4	Requirements Compliance	Based on at least yearly conducted compliance audit, verifications regarding relevant standards, regulations, legal/contractual, and statutory requirements are audited.
2.5	Audit Management Process	oculavis implements a formal and documented audit management process to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports.
2.6	Remediation	Based on the formal audit process, oculavis maintains a risk-based corrective action plan to remediate audit findings in a documented way. This also includes the involvement of all relevant stakeholders.
3. Application & Interface Security		

3.1	Application and Interface Security Policy and Procedures	Based on ISO 27001 requirements, our policies and regulations are audited by an external auditor on an annual basis. Application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities. Similarly, application security policies and procedures are reviewed and updated at least annually.
3.2	Application Security Baseline Requirements	Based on ISO 27001, baseline requirements to secure different applications are established, documented, and maintained.
3.3	Application Security Metrics	Based on ISO 27001, technical and operational metrics are defined and implemented according to business objectives, security requirements, and compliance obligations.
3.4	Secure Application Design and Development	Based on ISO 27001, SDLC process is defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements.
3.5	Automated Application Security Testing	Testing strategy does outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals. Moreover, testing is automated when applicable and possible. Internal penetration tests are carried out before new releases of the software products. Internal audit documents are not freely available, but any fixed vulnerabilities found are documented in the release notes.
3.6	Automated Secure Application Deployment	Strategies and capabilities are established and implemented to deploy application code in a secure, standardized, and compliant manner. The deployment and integration of application code is automated where possible.
3.7	Application Vulnerability Remediation	Application security vulnerabilities remediation process is following defined processes and the remediation of application security vulnerabilities is automated when possible.

4. Business Continuity Management and Operational Resilience

4.1	Business Continuity Management Policy and Procedures	Based on the business impact analysis, a framework for planning the business continuity and a business continuity plan is introduced, documented and applied with clear roles & responsibilities, defined communication channels, restoration procedures & recovery time targets, temporary intermediate solutions and improvement processes as well as integration of the incident management.
4.2	Risk Assessment and Impact Analysis	A risk management system has been implemented which regularly (in general on an annual basis) analyzes risks and weaknesses, derives suitable measures, and monitors the overall status (PDCA cycle). Key stakeholders are involved within the risk assessment with clear responsibilities.
4.3	Business Continuity Strategy	The overall business continuity management (BCM) strategy involves planning, implementing, and testing the business continuity concept as well as incorporating safeguards to ensure and maintain operations including regularly (in general on an annual basis) verification, reviews, and updates.
4.4	Business Continuity Planning	Operational resilience strategies and capability results are incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan.

4.5	Documentation	Based on ISO 27001, relevant documentation is developed, identified, and acquired to support business continuity and operational resilience plans. Moreover, business continuity and operational resilience documentation is available to authorized stakeholders and business continuity and operational resilience documentation are reviewed regularly.
4.6	Business Continuity Exercises	The business continuity and operational resilience plans are exercised and tested at least annually and when significant changes are applied- All BCM exercises are documented.
4.7	Communication	Business continuity and resilience procedures establish communication with stakeholders and participants during the management review meeting.
4.8	Backup	Cloud data is periodically backed up, the confidentiality, integrity, and availability of backup data is ensured and backups can be restored appropriately for resiliency. Backup and recovery policies and procedures are implemented. The servers and databases are regularly backed up and checked in accordance with the SLA. SLA Basic: Weekly backup of the oculavis' software products with a retention period of 4 weeks. SLA Standard/Premium: Daily backup of the oculavis' software products with a retention period of 7 days. Weekly backup of the oculavis' software products with a retention period of 4 weeks. Monthly backup of the oculavis' software products with a retention period of 12 months. Older backups are deleted step by step. Microsoft Azure backup: https://azure.microsoft.com/en-us/products/backup/ T-Systems Open Telekom Cloud backup: https://www.open-telekom-cloud.com/en/products-services/core-services/cloud-server-backup-service
4.9	Disaster Response Plan	There exists a disaster response plan how to immediately act in case of an incident. After a security/data privacy incident has been identified, a documentation, an analysis and an evaluation of the security/data privacy incident are performed. Measures are then taken and in the event of a customer-relevant incident, the customer is informed of the incident via Email/phone and the measures within 24 hours.
4.10	Response Plan Exercise	The emergency response plan is exercised annually or when significant changes occur and in case local emergency authorities are included, if possible, in the exercise.
4.11	Equipment Redundancy	Business-critical equipment is supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.
5. Change Control and Configuration Management		
5.1	Change Management Policy and Procedures	A formal change management process exists at oculavis GmbH, especially in the area of software development and deployment (customer instances). Requests for changes are formally entered in the backlog via the product owner. This is followed by a priority assessment, a technical classification and security assessment of the change, and a rough time estimate. Changes implemented are developed/deployed and intensively tested within sprints and there is a formal review process, especially for security-related changes.
5.2	Quality Testing	A defined quality change control, approval and testing process (with established baselines, testing, and release standards) is followed.
5.3	Change Management Technology	Risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) are managed, regardless of whether asset management occurs internally or externally (i.e., outsourced).
5.4	Unauthorized Change Protection	The unauthorized addition, removal, update, and management of organization assets is restricted and only performed by authorized employees.
5.5	Change Agreements	Provisions to limit changes that directly impact customer’s environments and require customers to authorize requests explicitly included within the service level agreements (SLAs) between oculavis and customers.

5.6	Change Management Baseline	Change management baselines are established for all relevant authorized changes on organizational assets; as in alignment with ISO 27001.
5.7	Detection of Baseline Deviation	Detection measures are implemented with proactive notification if changes deviate from established baselines.
5.8	Exception Management	oculavis implemented an emergency change process for exception management.
5.9	Change Restoration	Based upon our backup policy, a process to proactively roll back changes to a previously known "good state" is defined and implemented in case of errors or security concerns.
6. Cryptography, Encryption & Key Management (CEK)		
6.1	Encryption and Key Management Policy and Procedures	oculavis GmbH has a key and certificate management concept with a clear authorization/generation concept and according to BSI-Recommendation BSI TR-02102. Within projects, oculavis will follow the cryptographic requirements specified in BSI TR-03116. The key generation and CSR process is integrated into the automated deployment of the software products, which is configured by the software's administrators' group. All access to confidential keying material or certificates is controlled by the data protection officer.
6.2	Roles and Responsibilities	Cryptography, encryption, and key management roles and responsibilities are defined and implemented based on the need to know principle.
6.3	Data Encryption	Use of encryption to store personal and confidential data. Encryption of personal data during transport on mobile data carriers (laptops, desktop computers, hard disks, USB sticks) is also implemented following approved encryption algorithms.
6.4	Encryption Algorithm	oculavis uses SHA-256 Salted Hash values for storing passwords. (Virtual) disks and backups are encrypted using AES-256 encryption algorithm.
6.5	Encryption Change Management	Standard change management procedures are established to review, approve, implement, and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources.
6.6	Encryption Change Cost Benefit Analysis	Changes to cryptography, encryption and key management related systems, policies, and procedures are managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.
6.7	Encryption Risk Management	Cryptography, encryption, and key management are part of the oculavis risk management process.
6.8	Key Management Capability	The cloud service providers utilized by oculavis are providing oculavis with the capacity to manage their own data encryption keys.
6.9	Encryption and Key Management Audit	Encryption and key management systems, policies, and processes are audited with a frequency proportional to the system's risk exposure, and after any security event. Audit is done at least annually.
6.10	Key Generation	Cryptographic keys are generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications.

6.11	Key Purpose	Private keys are provisioned for a unique purpose.
6.12	Key Rotation	Private keys are rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements.
6.13	Key Revocation	Cryptographic keys are revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions.
6.14	Key Destruction	Processes, procedures, and technical measures to destroy unneeded keys are defined, implemented, and evaluated.
6.15	Key Activation	Processes, procedures, and technical measures to create keys are being defined, implemented, and evaluated to include legal and regulatory requirement provisions.
6.16	Key Suspension	Processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) are being defined, implemented, and evaluated to include legal and regulatory requirement provisions.
6.17	Key Deactivation	Processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) are being defined, implemented, and evaluated to include legal and regulatory requirement provisions.
6.18	Key Archival	If needed, encryption keys are archived. Processes, procedures, and technical measures to manage archived keys are being defined.
6.19	Key Compromise	Processes, procedures, and technical measures to handle compromised keys are implemented and included to the risk management of oculavis.
6.20	Key Recovery	Backup processes, procedures, and technical measures to assess operational continuity risks are being defined, implemented, and evaluated.
6.21	Key Inventory Management	Key management system processes, procedures, and technical measures are being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirement provisions.
6.22	Encryption of transmission	Encryption during the online transmission of personal data. Encryption of video streams, encrypted connection to software platform oculavis SHARE (DTLS 1.2, SRTP, HTTPS, TLS 1.2).

7. Data Security and Privacy Lifecycle Management

7.1	Security and Privacy Policy and Procedures	Policies and procedures are established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level. Internal privacy and IT security policies (based on the ISMS ISO 27001 Norm), including procedures under applicable laws and regulations, are implemented and regularly (in general on an annual basis) reviewed and updated, as necessary.
7.2	Secure Disposal	Industry-accepted methods are applied for secure data disposal from storage media so information is not recoverable by any forensic means.
7.3	Data Inventory	Use of encryption to store personal data. Passwords saved as Salted Hash (SHA-256). Databases and customer data in the file system are encrypted (AES-256). Backups are also encrypted (AES-256). Regular internal audits (in general on an annual basis) to verify compliance with data protection and IT security policies and to assess whether they are appropriate to ensure the protection of personal data. Internal penetration tests are carried out before new releases of the oculavis' software products. Internal audit documents are not freely available, but any fixed vulnerabilities found are documented in the release notes.
7.4	Data Classification	Data is classified according to type and sensitivity levels. All employees are aware of the data classification and of the handling procedure.

7.5	Data Flow Documentation	Data flow documentation is created to identify what data is processed and where it is stored and transmitted. The documentation is reviewed at defined intervals, at least annually, and after any change.
7.6	Data Ownership and Stewardship	The ownership and stewardship of all relevant personal and sensitive data is documented in an asset inventory and reviewed at least annually.
7.7	Data Protection by Design and Default	Systems, products, and business practices are based on security principles by design and per industry best practices.
7.8	Data Privacy by Design and Default	oculavis has appointed a data protection officer for implementing, monitoring and advising data protection topics.
7.9	Data Protection Impact Assessment	A data protection impact assessment (DPIA) is conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices. Processes, procedures, and technical measures are defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations).
7.10	Sensitive Data Transfer	Processes, procedures, and technical measures are defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per GDPR). Processes, procedures, and technical measures are defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject).
7.11	Personal Data Access, Reversal, Rectification and Deletion	Processes, procedures, and technical measures are defined, implemented, and evaluated for the transfer and sub-processing of personal data (according to GDPR regulations). Processes, procedures, and technical measures are defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation. Access to personal (customer) data by oculavis employees is subject to corresponding confidentiality obligations (employment contract and confidentiality agreement, in particular with regard to handling customer data). oculavis stores personal data only for the operation of business operations. Customer data is accessed after getting consent of the customer and accessed with four eyes principle. A deletion concept has been implemented which guarantees retention periods for personal data. An automatic or semi-automatic deletion of personal data does not take place during the contract period. At the end of the contract, the customer is given the opportunity to save data from his software platform oculavis SHARE. All personal data will be deleted and/or destroyed in a controlled manner at the end of the retention period (usually 90 days) or at the request of the customer. Log files are deleted after 30 day.
7.12	Limitation of Purpose in Personal Data Processing	Authorization from data owners is obtained, and the associated risk is managed, before replicating or using production data in non-production environments. Data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations.
7.13	Personal Data Sub-processing	Processes, procedures, and technical measures are defined, implemented, and evaluated for the transfer and sub-processing of personal data (according to GDPR).

7.14	Disclosure of Data Sub-Processors	Processes, procedures, and technical measures are defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation.
7.15	Limitation of Production Data Use	Authorization from data owners is obtained, and the associated risk is managed, before replicating or using production data in non-production environments.
7.16	Sensitive Data Protection	Processes, procedures, and technical measures are defined and implemented to protect sensitive data throughout its lifecycle as per GDPR.
7.17	Disclosure Notification	oculavis' cloud service providers describe to oculavis, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations.
7.18	Data Location	Processes, procedures, and technical measures are defined and implemented to specify and document physical data locations, including locales where data is processed or backed up.
8. Governance, Risk and Compliance		
8.1	Governance Program Policy and Procedures	Information governance program policies and procedures sponsored by organizational leadership are established, documented, approved, communicated, applied, evaluated, and maintained and updated at least annually.
8.2	Risk Management Program	oculavis has an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.
8.3	Organizational Policy Reviews	Annual review, assessment, and evaluation of the effectiveness of the technical and organizational measures is anually performed and as well an annual review of compliance with data protection and IT security guidelines by the data protection and IT security officer is performed.
8.4	Policy Exception Process	An approved exception process is mandated by the governance program established at oculavis and followed whenever a deviation from an established policy occurs.
8.5	Information Security Program	Initial training of new employees in the areas of information security through workshops on the subject of IT security and data protection.
8.6	Governance Responsibility Model	Roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs are defined and documented.
8.7	Information System Regulatory Mapping	Based on ISO 27001, all relevant standards, regulations, legal/contractual, and statutory requirements are identified and documented at oculavis.
8.8	Special Interest Groups	At oculavis, contact is established and maintained with cloud-related special interest groups and other relevant entities.
9. Human Resources		

9.1	Background Screening Policy and Procedures	Background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) are established, documented, approved, communicated, applied, evaluated, and maintained. Background verification policies and procedures are designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk. Background verification policies and procedures are reviewed and updated at least annually.
9.2	Acceptable Use of Technology Policy and Procedures	Policies and procedures for defining allowances and conditions for the acceptable use of organizationally or managed assets are established, documented, approved, communicated, applied, evaluated, maintained, and updated at least annually.
9.3	Clean Desk Policy and Procedures	Policies and procedures requiring unattended workspaces to conceal confidential data are established, documented, approved, communicated, applied, evaluated, maintained, and updated at least annually.
9.4	Remote and Home Working Policy and Procedures	Policies and procedures to protect information accessed, processed, or stored at remote sites and locations are established, documented, approved, communicated, applied, evaluated, maintained, and updated at least annually.
9.5	Asset returns	Return procedures of organizationally owned assets by terminated employees are established and documented.
9.6	Contract documents	Contractual obligations (confidentiality agreement) in the handling of customer data for all oculavis employees.
9.7	Employment Termination	Procedures outlining the roles and responsibilities concerning changes in employment are established, documented, and communicated to all personnel.
9.8	Employment Agreement Process	Employees are required to sign an employment agreement before gaining access to organizational information systems, resources, and assets.
9.9	Employment Agreement Content	Provisions and/or terms for adherence to established information governance and security policies are included within employment agreements.
9.10	Personnel Roles and Responsibilities	Employee roles and responsibilities relating to information assets and security are documented and communicated.
9.11	Non-Disclosure Agreements	Requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details are identified, documented, and reviewed at planned intervals.
9.12	Security Awareness Training	Regular training of employees in the areas of data protection and IT security through bi-weekly company meetings on the subject of IT security and data protection.
9.13	Compliance User Responsibility	Employees are notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations.
10. Identity & Access Management		

10.1	Identity and Access Management Policy and Procedures	Access to personal (customer) data by oculavis employees is subject to corresponding confidentiality obligations (employment contract and confidentiality agreement, in particular about handling customer data).
10.2	Strong Password Policy and Procedures	Strong password policies and procedures are established, documented, approved, communicated, implemented, applied, evaluated maintained and updated at least annually.
10.3	Identity Inventory	System identity information and levels of access is managed, stored, and reviewed.
10.4	Separation of Duties	The separation of duties principle is employed when implementing information system access.
10.5	Least Privilege	Authorizations and accesses are assigned and granted based on the need-to-know principle, taking into account the sensitivity and criticality of data processing, and the employee's responsibilities within the company. Authorizations and accesses are assigned and granted on the basis of the need-to-know principle, taking into account the sensitivity and criticality of data processing, and the employee's responsibilities within the company.
10.6	User Access Provisioning	A user access provisioning process is defined and implemented which authorizes, records, and communicates data and assets access changes.
10.7	User Access Changes and Revocation	A process is in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies.
10.8	User Access Review	Reviews and revalidation of user access for least privilege and separation of duties are completed with a frequency commensurate with organizational risk tolerance.
10.9	Segregation of Privileged Access Roles	Processes, procedures, and technical measures for the segregation of privileged access roles are defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate.
10.10	Management of Privileged Access Roles	An access process is defined and implemented to ensure privileged access roles and rights are granted for a limited period. Procedures implemented to prevent the culmination of segregated privileged access.
10.11	Safeguard logs Integrity	Processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all (including privileged access roles) are defined, implemented, and evaluated. The ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties.
10.12	Uniquely Identifiable Users	Processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) are defined, implemented, and evaluated.
10.13	Strong Authentication	Processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multi factor authentication for a least-privileged user and sensitive data access are defined, implemented, and evaluated. Digital certificates or alternatives that achieve an equivalent security level for system identities are adopted.

10.14	Passwords Management	Processes, procedures, and technical measures for the secure management of passwords are defined, implemented, and evaluated.
10.15	Authorization Mechanisms	Processes, procedures, and technical measures to verify access to data and system functions are authorized, defined, implemented, and evaluated.

11. Infrastructure & Virtualization Security

11.1	Capacity and Resource Planning	Resource availability, quality, and capacity are planned and monitored in a way that delivers required system performance, as determined by the business.
11.2	Network Security	Communications between environments are monitored and encrypted. The protection of the internal network against unauthorized access is ensured by a security gateway with firewall and IDS module. Network configurations are reviewed at least annually and supported by the documented justification of all allowed services, protocols, ports, and compensating controls.
11.3	Production and Non-Production Environments	The software platform for the client runs on its own customer instance and is completely isolated from other customer instances. Furthermore, the platform is divided into modules and deployed according to the docker concept (sandbox concept), so that the individual modules (database, frontend, backend) are additionally isolated.
11.4	Segmentation and Segregation	Strict separation of test/development data/platforms and production data/platforms. Only the software’s Administrators Group has access to the customer instances (production environment) and only for backup, update, or data recovery purposes. Anomalies in the access are handled by the Incident Management of oculavis.
11.5	Migration to Cloud Environments	oculavis has implemented secure and encrypted communication channels including only up-to-date and approved protocols are used when migrating servers, services, applications, or data to cloud environments.
11.6	Network Architecture Documentation	Identification and documentation of high-risk environments.
11.7	Network Defense	Processes, procedures, and defense techniques are defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks.
11.8	Asset Management	Assets associated with information and information processing facilities are identified and an inventory of these assets is drawn up with clear responsibilities and regularly (in general on an annual basis) maintained. All information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. A set of procedures for information labelling and handling is implemented according to the information classification scheme.
11.9	Security gateway	The protection of the internal network against unauthorized access is ensured by a security gateway with firewall and IDS module.

12. Logging and Monitoring

12.1	Logging and Monitoring Policy and Procedures	Logging and monitoring policies and procedures are established, documented, approved, communicated, applied, evaluated, maintained and updated at least annually. A pseudonymized logging of all data accesses with timestamps to instances of the client takes place. Log files can only be viewed by administrators and are protected against unauthorized manipulation. The assignment of authorizations is documented in detail by full name. The data protection officer monitors the authorized persons accesses on instances of the client. Log files in the background of the software document system adjustments and serve to prevent error states, detect potential attacks on the system and ensure traceability of system activities.
12.2	Audit Logs Protection	Processes, procedures, and technical measures are defined, implemented, and evaluated to ensure audit log security and retention. The data protection officer monitors the authorized persons accesses on instances of the client.
12.3	Security Monitoring and Alerting	Security-related events are identified and monitored within applications and the underlying infrastructure. A process is defined and implemented to communicate alerts to responsible stakeholders based on security events and their corresponding metrics.
12.4	Audit Logs Access and Accountability	Access to audit logs is restricted to authorized personnel, and records are maintained to provide unique access accountability.
12.5	Audit Logs Monitoring and Response	Security audit logs are monitored to detect activity outside of typical or expected patterns. Process is established and followed to review and take appropriate and timely actions on detected anomalies.
12.6	Clock Synchronization	A reliable time source is being used across all relevant information processing systems.
12.7	Log Protection	The information system protects log records from unauthorized access, modification, and deletion.
12.8	Access Control Logs	Physical access is logged and monitored using an auditable access control system.
12.9	Failures and Anomalies Reporting	Processes and technical measures for reporting monitoring system anomalies and failures are defined, implemented, and evaluated. Accountable parties are immediately notified about anomalies and failures.

13. Security Incident Management, E-Discovery, & Cloud Forensics

13.1	Security Incident Management Policy and Procedures	Policies and procedures for security incident management, e-discovery and cloud forensics are established, documented, approved, communicated, applied, evaluated, maintained, reviewed, and updated annually.
13.2	Service Management Policy and Procedures	Policies and procedures for timely management of security incidents are established, documented, approved, communicated, applied, evaluated, maintained, reviewed, and updated at least annually.
13.3	Incident Response Plans	There exists an emergency response plan how to immediately act in case of an incident. After a security/data privacy incident has been identified, a documentation, an analysis and an evaluation of the security/data privacy incident are performed. Measures are then taken and in the event of a customer-relevant incident, the customer is informed of the incident via E-Mail/phone and the measures within 24 hours.

13.4	Incident Response Testing	The security incident response plan is tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes.
13.5	Incident Response Metrics	Information security incident metrics are established and monitored.
13.6	Security Breach Notification	Processes, procedures, and technical measures for security breach notifications are defined and implemented. Security breaches and assumed security breaches are reported (including any relevant supply chain breaches).
13.7	Points of Contact Maintenance	Points of contact is maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

14. Supply Chain Management, Transparency, and Accountability

14.1	SSRM Policy and Procedures	Policies and procedures implementing the shared security responsibility model (SSRM) within the organization are established, documented, approved, communicated, applied, evaluated, maintained, reviewed, and updated annually.
14.2	Supply Chain Risk Management	Risk factors are associated with all organizations within the supply chain periodically reviewed by oculavis.
14.3	Primary Service and Contractual Agreement	Service agreements between oculavis and customers (tenants) incorporate at least the following mutually agreed upon provisions and/or terms. ◆ Scope, characteristics, and location of business relationship and services offered ◆ Information Technology requirements ◆ Logging and monitoring capability ◆ Incident management and communication procedures ◆ Right to audit and third-party assessment ◆ Service termination ◆ Interoperability and portability requirements ◆ Data privacy
14.4	Internal Compliance Testing	Based on ISO 27001, there is a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities.
14.5	Supply Chain Data Security Assessment	A process to conduct security assessments for all supply chain organizations is defined and implemented.
14.6	Subcontractor s	There is a clear process for selecting subcontractors. Formalized, documented, and controlled data processing agreements have been concluded with the subcontractors commissioned by oculavis GmbH and all sub processors are regularly checked. Data protection-compliant data processing agreements with subcontractors through concluded EU standard contract clauses.
14.7	Responsibilitie s	Clear distinction between the areas of responsibility of the client and the contractor.

14.8	Procurement process	Procurement of hardware and software is centralized. All procurements are inventoried.

15. Threat & Vulnerability Management

15.1	Threat and Vulnerability Management Policy and Procedures	Policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation. Threat and vulnerability management policies and procedures are reviewed and updated at least annually.
15.2	Malware Protection Policy and Procedures	Policies and procedures to protect against malware on managed assets are established, documented, approved, communicated, applied, evaluated, maintained, reviewed, and updated at least annually.
15.3	Vulnerability Remediation Schedule	Processes, procedures, and technical measures are defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk).
15.4	Detection Updates	Processes, procedures, and technical measures are defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators on frequent basis.
15.5	External Library Vulnerabilities	Processes, procedures, and technical measures are defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the oculavis' vulnerability management policy).
15.6	Penetration Testing	Internal penetration tests are carried out before new releases of the oculavis' software products. Internal audit documents are not freely available, but any fixed vulnerabilities found are documented in the release notes.
15.7	Vulnerability Identification	Processes, procedures, and technical measures are defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly.
15.8	Vulnerability Prioritization	Vulnerability remediation is prioritized using a risk-based model from an industry-recognized framework.
15.9	Vulnerability Management Reporting	A process is defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification.
15.10	Vulnerability Management Metrics	Metrics for vulnerability identification and remediation are established, monitored, and reported at defined intervals.

16. Universal Endpoint Management

16.1	Endpoint Devices Policy and Procedures	Policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints. Universal endpoint management policies and procedures are reviewed and updated at least annually.
16.2	Application and Service Approval	There is a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.
16.3	Compatibility	A process is defined and implemented to validate endpoint device compatibility with operating systems and applications.

16.4	Endpoint Inventory	An inventory of all endpoints is used and maintained to store and access company data.
16.5	Endpoint Management	Processes, procedures, and technical measures are defined, implemented, and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.
16.6	Automatic Lock Screen	All relevant interactive-use endpoints are configured to require an automatic password protected lock screen.
16.7	Operating Systems	Changes to endpoint operating systems, patch levels, and/or applications are managed through the organizational change management process.
16.8	Storage Encryption	Information is protected from unauthorized disclosure on managed endpoints with storage encryption.
16.9	Anti-Malware Detection and Prevention	If based on the oculavis' risk management needed, malware detection and prevention technology services are configured on managed endpoints.
16.10	Software Firewall	Software firewalls are configured on managed endpoints.
16.11	Data Loss Prevention	Managed endpoints are configured with data loss prevention (DLP) technologies and rules are defined based on a risk assessment.
16.12	Remote Locate	Remote geolocation capabilities are enabled for all managed mobile endpoints.
16.13	Remote Wipe	Processes, procedures, and technical measures are defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices.
16.14	Third-Party Endpoint Security Posture	Processes, procedures, and technical and/or contractual measure are defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets.
17. Software Product		
17.1	Software Release Process	There is a formal release procedure for software versions of oculavis SHARE and data protection and IT security requirements are part of the software release process. Releases are delivered every 6-8 weeks.
17.2	License management	No installation of third-party software without license rights. A list of libraries/dependencies together with their licensing information is maintained for oculavis SHARE and is reviewed/updated regularly (part of the software release process).
17.3	Patch management	Updating of all software and IT used in connection with data processing (e.g., through updates, patches, fixes, etc.). A patch and vulnerability management exists at oculavis GmbH, especially a monitoring for available (security) patches of relevant used libraries/systems. Patches are applied promptly and libraries are kept up to date. Typically patches for oculavis SHARE are delivered every 6-8 weeks. Depending on the severity and BSI recommendation, security patches may also be fixed earlier and applied as "hot fixes" (typically within four weeks after publication of an update/vulnerability).
17.4	Change Management	A formal change management process exists at oculavis GmbH, especially in the area of software development and deployment (customer instances). Requests for changes are formally entered in the backlog via the product owner. This is followed by a priority assessment, a technical classification and security assessment of the change, and a rough time estimate. Changes implemented are developed/deployed and intensively tested within sprints and there is a formal review process, especially for security-related changes.

17.5	Remote support	Guidelines for remote maintenance and support have been implemented.
17.6	Secure Scrum	IT security is part of the agile development process of the software oculavis SHARE according to 4 phase model: • Planning und Analyse (Backlog) • Secure implementation • Verification and security testing • Security-Gate as part of the DoD
17.7	oculavis SHARE Administrators	SHARE administrators receive regular training on how to use confidential authenticators (passwords, keys, etc.), how to utilize privileged access, and how to act with their special role and responsibility.
17.8	Secure coding	Regular (at job start and then at least yearly) training on Secure Scrum development and secure coding based on the OWASP recommendations for all software developers of oculavis SHARE.
17.9	Regular review	Regular review, assessment, and evaluation of the effectiveness of the technical and organizational measures as well as regular review of compliance with data protection and IT security guidelines by the data protection and IT security officer.
17.10	Input validation	User input is strictly validated to prevent injection attacks (e.g., SQL injections or XSS).
17.11	Logging	A pseudonymized logging of all data accesses with timestamps to instances of the client takes place. Log files can only be viewed by administrators and are protected against unauthorized manipulation. The assignment of authorizations is documented in detail by full name. The data protection officer monitors the authorized persons accesses on instances of the client. Log files in the background of the software document system adjustments and serve to prevent error states, detect potential attacks on the system and ensure traceability of system activities.
17.12	Monitoring	The customer instances and the IT infrastructure of oculavis GmbH are monitored to detect anomalies, potential malicious activities or server downtimes.

18. Physical Security

18.1	Alarm	Alarm-monitored building, office space and separately secured server room.
18.2	Security token	Use of personal security tokens for access to the building and office premises, including access logging.
18.3	Access permissions	oculavis has implemented physical access authorizations for employees and third parties (visitors, customers, cleaning personnel, craftsmen, etc.), including the request, authorization, and removal of access.
18.4	Secured server room	Separate key system for the server room with sharp-name assignment of access authorizations and logging of accesses. The access protection to the server farms of our hosting providers depends on the physical security measures of the hosting provider.
18.5	Management of media devices	Procedures are implemented for the management of media/removable media in accordance with the classification scheme. Media shall be disposed of securely when no longer required, using these formal procedures.

19. Interoperability & Portability

19.1	Interoperability and Portability Policy and Procedures	Policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs), information processing interoperability, application development portability, information/data exchange, usage, portability, integrity, and persistence. These policies and procedures are reviewed and updated at least annually.

19.2	Application Interface Availability	oculavis can programmatically retrieve data via an application interface to enable interoperability and portability.
19.3	Secure Interoperability and Portability Management	Cryptographically secure and standardized network protocols are implemented for the management, import, and export of data.