Technische und organisatorische Maßnahmen (TOMs) gemäß Art. 28 DSGVO, Stand 14.08.2023

Dieses Kapitel beschreibt die technischen und organisatorischen Maßnahmen, die von oculavis SHARE Software, oculavis SHARE Apps und des Entwicklungsunternehmens oculavis GmbH umgesetzt werden. Diese Maßnahmen sind verbindlich und gelten für alle Fälle von Datenverarbeitungstätigkeiten. Die getroffenen Maßnahmen berücksichtigen den Stand der Technik gemäß den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und den Empfehlungen des IT-Sicherheitsverbandes Deutschland.
Der Datenschutzbeauftragte der oculavis GmbH sichert die Erfüllung der TOMs zu und gewährleistet auf Dauer, dass die gewählten technischen und organisatorischen Maßnahmen für die vorliegende Datenverarbeitung durch die oculavis GmbH in Kraft bleiben.

ID	Maßnahme	Beschreibung
1. Bescheinigungen		
1.1	Zertifizierungen	oculavis ist ISO 27001 zertifiziert, darüber hinaus verfügen die Hosting-Provider von oculavis über mehrere Zertifizierungen, siehe auch: • Microsoft: https://azure.microsoft.com/de-de/explore/trusted-cloud/compliance/ • T-Systems: https://www.open-telekom-cloud.com/de/produkte-services/core-services/zertifikate
1.2	Hosting-Anbieter	Wir unterstützen derzeit die folgenden Hosting Provider mit den entsprechenden technischen und organisatorischen Sicherheitsmaßnahmen: • Microsoft: https://docs.microsoft.com/de-de/azure/security/ • T-Systems: https://www.telekom.com/en/corporateresponsibility/data- protection-datasecurity/security/details/privacy-and-securityassessment-process-358312
2. Prüfung und Sicherheit		
2.1	Prüfungs- und Sicherheits-Politik und -Verfahren	Interne Datenschutz- und IT-Sicherheitsrichtlinien (auf der Grundlage der ISMS-Norm ISO27001), einschließlich der Verfahren gemäß den geltenden Gesetzen und Vorschriften, werden umgesetzt und regelmäßig (in der Regel jährlich) überprüft und bei Bedarf aktualisiert.

2.2	Unabhängige Beurteilungen	Auf der Grundlage der ISO 27001-Anforderungen werden unsere Richtlinien und Vorschriften jährlich von einem externen Prüfer geprüft.
2.3	Risikobasierte Planungsbewertung	Auf der Grundlage des Risikomanagements werden die internen Systeme und ihre Verantwortlichen zusätzlich überwacht und geprüft.
2.4	Einhaltung der Anforderungen	Auf der Grundlage eines mindestens jährlich durchgeführten Compliance-Audits wird die Einhaltung relevanter Normen, Vorschriften, rechtlicher/vertraglicher und gesetzlicher Anforderungen geprüft.
2.5	Audit-Management- Prozess	oculavis implementiert einen formalen und dokumentierten Audit-Management-Prozess zur Unterstützung der Audit-Planung, der Risikoanalyse, der Bewertung der Sicherheitskontrollen, der Schlussfolgerungen, der Zeitpläne für Abhilfemaßnahmen, der Erstellung von Berichten und der Überprüfung früherer Berichte.
2.6	Sanierung	Auf der Grundlage des formalen Auditprozesses unterhält oculavis einen risikobasierten Korrekturmaßnahmenplan, um die Auditfeststellungen auf dokumentierte Weise zu beheben. Dazu gehört auch die Einbeziehung aller relevanten Interessengruppen.
3. Sicherheit von Anwendungen und Schnittstellen		
3.1	Sicherheitspolitik und verfahren für Anwendungen und Schnittstellen	Auf der Grundlage der Anforderungen von ISO 27001 werden unsere Richtlinien und Vorschriften jährlich von einem externen Prüfer kontrolliert. Richtlinien und Verfahren für die Anwendungssicherheit werden erstellt, dokumentiert, genehmigt, kommuniziert, angewandt, bewertet und gepflegt, um eine angemessene Planung, Bereitstellung und Unterstützung der Anwendungssicherheitsfunktionen der Organisation zu gewährleisten. Ebenso werden die Richtlinien und Verfahren für die Anwendungssicherheit mindestens einmal jährlich überprüft und aktualisiert.

3.2	Grundlegende Anforderungen an die Anwendungssicherheit	Auf der Grundlage von ISO 27001 werden grundlegende Anforderungen an die Sicherheit verschiedener Anwendungen festgelegt, dokumentiert und gepflegt.
3.3	Metriken zur Anwendungssicherheit	Auf der Grundlage von ISO 27001 werden technische und betriebliche Metriken definiert und entsprechend den Geschäftszielen, Sicherheitsanforderungen und Compliance Verpflichtungen umgesetzt.
3.4	Design und Entwicklung sicherer Anwendungen	Auf der Grundlage von ISO 27001 wird ein SDLC-Prozess für den Entwurf, die Entwicklung, den Einsatz und den Betrieb von Anwendungen gemäß den Sicherheitsanforderungen des Unternehmens definiert und implementiert.
3.5	Automatisierte Tests der Anwendungssicherheit	Die Teststrategie enthält Kriterien für die Annahme neuer Informationssysteme, Upgrades und neuer Versionen und gewährleistet gleichzeitig die Anwendungssicherheit, die Einhaltung von Vorschriften und die Einhaltung der organisatorischen Ziele für eine schnelle Bereitstellung. Außerdem werden die Tests, wenn möglich, automatisiert. Interne Penetrationstests werden vor neuen Versionen von Softwareprodukten durchgeführt. Die Dokumente der internen Prüfungen sind nicht frei zugänglich, aber alle behobenen Schwachstellen werden in den Versionshinweisen dokumentiert.
3.6	Automatisierte sichere Anwendungsbereitstellung	Es werden Strategien und Fähigkeiten entwickelt und implementiert, um den Anwendungscode auf sichere, standardisierte und konforme Weise bereitzustellen. Die Bereitstellung und Integration des Anwendungscodes werden nach Möglichkeit automatisiert.
3.7	Behebung von Anwendungsschwachstellen	Der Prozess zur Behebung von Sicherheitslücken in Anwendungen folgt definierten Prozessen, und die Behebung von Sicherheitslücken in Anwendungen wird nach Möglichkeit automatisiert.
4. Geschäftskontinuitätsmanagement und betriebliche Widerstandsfähigkeit		

4.1	Grundsätze und Verfahren für das Management der Geschäftskontinuität	Auf der Grundlage der Analyse der Auswirkungen auf das Geschäft wird ein Rahmen für die Planung der Geschäftskontinuität und ein Geschäftskontinuitätsplan mit klaren Rollen und Verantwortlichkeiten, definierten Kommunikationskanälen, Wiederherstellungsverfahren und Wiederherstellungszeitzielen, vorübergehenden Zwischenlösungen und Verbesserungsprozessen sowie der Integration des Vorfallsmanagements eingeführt, dokumentiert und angewendet.
4.2	Risikobewertung und Folgenanalyse	Es wurde ein Risikomanagementsystem eingeführt, das regelmäßig (in der Regel jährlich) Risiken und Schwachstellen analysiert, geeignete Maßnahmen ableitet und den Gesamtstatus überwacht (PDCA-Zyklus). Die wichtigsten Interessengruppen sind mit klaren Zuständigkeiten an der Risikobewertung beteiligt.
4.3	Strategie der Geschäftskontinuität	Die Gesamtstrategie für das Business Continuity Management (BCM) umfasst die Planung, Umsetzung und Prüfung des Business-Continuity- Konzepts sowie die Einbeziehung von Schutzmaßnahmen zur Gewährleistung und Aufrechterhaltung des Betriebs, einschließlich regelmäßiger (in der Regel jährlicher) Verifizierung, Überprüfung und Aktualisierung.
4.4	Planung der Geschäftskontinuität	Operative Resilienzstrategien und Fähigkeitsergebnisse werden einbezogen, um einen Business-Continuity-Plan zu erstellen, zu dokumentieren, zu genehmigen, zu kommunizieren, anzuwenden, zu bewerten und zu pflegen.
4.5	Dokumentation	Auf der Grundlage von ISO 27001 werden relevante Unterlagen zur Unterstützung von Plänen für die Geschäftskontinuität und die betriebliche Widerstandsfähigkeit entwickelt, ermittelt und beschafft. Darüber hinaus ist die Dokumentation der Geschäftskontinuität und der operativen Belastbarkeit für autorisierte Interessengruppen verfügbar und die Dokumentation der Geschäftskontinuität und der operativen Belastbarkeit wird regelmäßig überprüft.
4.6	Übungen zur Geschäftskontinuität	Die Pläne zur Aufrechterhaltung des Geschäftsbetriebs und der betrieblichen Ausfallsicherheit werden mindestens einmal jährlich sowie bei wesentlichen Änderungen geübt und getestet.

4.7	Kommunikation	Die Verfahren zur Gewährleistung der Kontinuität des Geschäftsbetriebs und der Widerstandsfähigkeit stellen die Kommunikation mit den Interessengruppen und den Teilnehmern der Managementbewertung sicher.
4.8	Sicherung	Cloud-Daten werden regelmäßig gesichert, die Vertraulichkeit, Integrität und Verfügbarkeit der Sicherungsdaten wird gewährleistet und die Sicherungen können in angemessener Weise wiederhergestellt werden, um die Ausfallsicherheit zu gewährleisten. Es werden Sicherungs- und Wiederherstellungsrichtlinien und -verfahren umgesetzt. Die Server und Datenbanken werden regelmäßig gemäß dem SLA gesichert und überprüft. SLA Basic: Wöchentliche Sicherung der Softwareprodukte von oculavis mit einer Aufbewahrungsfrist von 4 Wochen. SLA Standard/Premium: Tägliche Sicherung der oculavis Softwareprodukte mit einer Aufbewahrungsfrist von 7 Tagen. Wöchentliche Sicherung der oculavis-Softwareprodukte mit einer Aufbewahrungsfrist von 4 Wochen. Monatliche Sicherung der oculavis Softwareprodukte mit einer Aufbewahrungsfrist von 12 Monaten. Ältere Backups werden nach und nach gelöscht. Microsoft Azure Sicherung: https://azure.microsoft.com/de-DE/products/backup/ T-Systems Open Telekom Cloud Sicherung: https://www.telekom.com/de/konzern/datenschutz-und-sicherheit/news/privacy-and-security-assessment-verfahren-342724
4.9	Katastrophenschutzplan	Es gibt einen Katastrophenschutzplan, wie im Falle eines Vorfalls sofort gehandelt werden kann. Nachdem ein Sicherheits-/Datenschutzvorfall identifiziert wurde, erfolgt eine Dokumentation, Analyse und Bewertung des Sicherheits-/Datenschutzvorfalls. Anschließend werden Maßnahmen ergriffen und im Falle eines kundenrelevanten Vorfalls wird der Kunde innerhalb von 24 Stunden per E-Mail/Telefon über den Vorfall und die Maßnahmen informiert.
4.10	Reaktionsplan-Übung	Der Notfallplan wird jährlich oder bei wesentlichen Änderungen geübt, wobei die lokalen Notfallbehörden nach Möglichkeit in die Übung einbezogen werden.

4.11	Redundanz der Ausrüstung	Geschäftskritische Geräte werden durch redundante Geräte ergänzt, die unabhängig voneinander in einem angemessenen Mindestabstand gemäß den geltenden Industriestandards aufgestellt sind.
5. Änderungskontrolle und Konfigurationsmanagement		
5.1	Politik und Verfahren für das Änderungsmanagement	Bei der oculavis GmbH existiert ein formaler Change Management Prozess, insbesondere im Bereich der Softwareentwicklung und Bereitstellung (Kundeninstanzen). Änderungswünsche werden über den Product Owner formell in das Backlog eingetragen. Es folgt eine Prioritätsbewertung, eine technische Einordnung und Sicherheitsbewertung der Änderung sowie eine grobe Zeitabschätzung. Umgesetzte Änderungen werden innerhalb von Sprints entwickelt/umgesetzt und intensiv getestet, und es gibt einen formalen Überprüfungsprozess, insbesondere für sicherheitsrelevante Änderungen.
5.2	Qualitätsprüfung	Es wird ein definierter Prozess zur Kontrolle, Genehmigung und Prüfung von Qualitätsänderungen (mit festgelegten Basislinien, Prüf- und Freigabestandards) eingehalten.
5.3	Technologie für Änderungsmanagement	Risiken, die mit der Veränderung von Unternehmensressourcen (einschließlich Anwendungen, Systemen, Infrastruktur, Konfiguration usw.) verbunden sind, werden verwaltet, unabhängig davon, ob die Verwaltung der Ressourcen intern oder extern (d. h. ausgelagert) erfolgt.
5.4	Schutz vor unbefugten Änderungen	Das unbefugte Hinzufügen, Entfernen, Aktualisieren und Verwalten von Vermögenswerten der Organisation ist eingeschränkt und wird nur von autorisierten Mitarbeitern durchgeführt.
5.5	Vereinbarungen ändern	Bestimmungen zur Begrenzung von Änderungen, die sich direkt auf die Kundenumgebungen auswirken, und die Anforderung, dass Kunden Anfragen explizit genehmigen müssen, sind in den Service Level Agreements (SLAs) zwischen oculavis und Kunden enthalten.

5.6	Baseline des Änderungsmanagements	Änderungsmanagement-Baselines werden für alle relevanten autorisierten Änderungen an den Unternehmensressourcen erstellt, wie in Übereinstimmung mit ISO 27001.
5.7	Erkennung von Basislinienabweichungen	Es werden Erkennungsmaßnahmen mit proaktiver Benachrichtigung durchgeführt, wenn Änderungen von den festgelegten Grundlinien abweichen.
5.8	Management von Ausnahmen	oculavis implementierte einen Notfalländerungsprozess für das Ausnahmemanagement.
5.9	Veränderung Wiederherstellung	Auf der Grundlage unserer Backup-Richtlinie wird ein Prozess zur proaktiven Rückführung von Änderungen auf einen zuvor bekannten „guten Zustand“ definiert und implementiert, falls Fehler oder Sicherheitsbedenken auftreten.
6. Kryptographie, Verschlüsselung und Schlüsselverwaltung (CEK)		
6.1	Richtlinien und Verfahren für Verschlüsselung und Schlüsselverwaltung	Die oculavis GmbH verfügt über ein Schlüssel- und Zertifikatsmanagementkonzept mit einem klaren Berechtigungs-/Erzeugungskonzept und gemäß der BSI-Empfehlung BSI TR-02102. Im Rahmen von Projekten wird oculavis die in der BSI TR-03116 spezifizierten kryptographischen Anforderungen einhalten. Der Schlüsselgenerierungs- und CSR-Prozess ist in die automatisierte Bereitstellung der Softwareprodukte integriert, die von der Administratorengruppe der Software konfiguriert wird. Jeder Zugang zu vertraulichem Schlüsselmaterial oder Zertifikaten wird vom Datenschutzbeauftragten kontrolliert.
6.2	Rollen und Zuständigkeiten	Die Rollen und Zuständigkeiten in den Bereichen Kryptografie, Verschlüsselung und Schlüsselverwaltung werden nach dem Grundsatz „Kenntnisnahme erforderlich“ definiert und umgesetzt.
6.3	Datenverschlüsselung	Verwendung von Verschlüsselung zur Speicherung persönlicher und vertraulicher Daten. Die Verschlüsselung personenbezogener Daten während des Transports auf mobilen Datenträgern (Laptops, Desktop-Computer, Festplatten, USB-Sticks) erfolgt ebenfalls nach anerkannten Verschlüsselungsalgorithmen.

6.4	Verschlüsselungsalgorithmus	oculavis verwendet SHA-256 Salted Hash-Werte für die Speicherung von Passwörtern. (Virtuelle) Festplatten und Backups werden mit dem Verschlüsselungsalgorithmus AES-256 verschlüsselt.
6.5	Verschlüsselung Change Management	Es werden Standardverfahren für die Änderungsverwaltung eingerichtet, um Änderungen an der Kryptografie-, Verschlüsselungs- und Schlüsselverwaltungstechnologie zu prüfen, zu genehmigen, zu implementieren und zu kommunizieren, wobei interne und externe Quellen berücksichtigt werden.
6.6	Verschlüsselung ändern Kosten-Nutzen-Analyse	Änderungen an Kryptographie-, Verschlüsselungs- und Schlüsselverwaltungssystemen, -richtlinien und -verfahren werden so gehandhabt und angenommen, dass die nachgelagerten Auswirkungen der vorgeschlagenen Änderungen vollständig berücksichtigt werden, einschließlich Restrisiko, Kosten- und Nutzenanalyse.
6.7	Risikomanagement bei Verschlüsselung	Kryptographie, Verschlüsselung und Schlüsselverwaltung sind Teil des Risikomanagementprozesses von oculavis.
6.8	Schlüsselmanagement Fähigkeit	Die von oculavis genutzten Cloud-ServiceProvider stellen oculavis die Möglichkeit zur Verfügung, ihre eigenen Datenverschlüsselungsschlüssel zu verwalten.
6.9	Prüfung von Verschlüsselung und Schlüsselverwaltung	Verschlüsselungs- und Schlüsselverwaltungssysteme, -richtlinien und -prozesse werden mit einer Häufigkeit, die dem Risiko des Systems entspricht, und nach jedem Sicherheitsvorfall geprüft. Die Prüfung wird mindestens einmal jährlich durchgeführt.
6.10	Schlüsselgenerierung	Die kryptografischen Schlüssel werden mit branchenweit anerkannten und zugelassenen kryptografischen Bibliotheken generiert, die die Stärke des Algorithmus und die Spezifikationen des Zufallszahlengenerators festlegen.
6.11	Hauptzweck	Private Schlüssel werden für einen bestimmten Zweck zur Verfügung gestellt.

6.12	Taste Rotation	Die privaten Schlüssel werden auf der Grundlage einer Kryptoperiode rotiert, die unter Berücksichtigung des Risikos der Offenlegung von Informationen sowie rechtlicher und regulatorischer Anforderungen berechnet wird.
6.13	Schlüsselentzug	Kryptografische Schlüssel werden vor Ablauf der festgelegten Kryptoperiode (wenn ein Schlüssel kompromittiert wird oder eine Einheit nicht mehr Teil der Organisation ist) per definierten, implementierten und evaluierten Prozessen, Verfahren und technischen Maßnahmen widerrufen und entfernt, um gesetzliche und regulatorische Bestimmungen zu berücksichtigen.
6.14	Zerstörung von Schlüsseln	Prozesse, Verfahren und technische Maßnahmen zur Vernichtung nicht benötigter Schlüssel werden definiert, umgesetzt und bewertet.
6.15	Schlüssel-Aktivierung	Prozesse, Verfahren und technische Maßnahmen zur Erstellung von Schlüsseln werden definiert, implementiert und evaluiert, um rechtliche und regulatorische Anforderungen zu berücksichtigen.
6.16	Schlüssel Aufhängung	Prozesse, Verfahren und technische Maßnahmen zur Überwachung, Überprüfung und Genehmigung wichtiger Übergänge (z. B. von einem Zustand zu/von einer Aussetzung) werden definiert, umgesetzt und bewertet, um rechtliche und regulatorische Anforderungen zu berücksichtigen.
6.17	Deaktivierung der Taste	Prozesse, Verfahren und technische Maßnahmen zur Deaktivierung von Schlüsseln (zum Zeitpunkt ihres Ablaufdatums) werden definiert, implementiert und evaluiert, um gesetzliche und regulatorische Bestimmungen zu berücksichtigen.
6.18	Schlüssel Archivierung	Bei Bedarf werden die Verschlüsselungsschlüssel archiviert. Prozesse, Verfahren und technische Maßnahmen zur Verwaltung archivierter Schlüssel werden derzeit festgelegt.
6.19	Schlüsselkompromiss	Prozesse, Verfahren und technische Maßnahmen zum Umgang mit kompromittierten Schlüsseln werden implementiert und in das Risikomanagement von oculavis einbezogen.
6.20	Schlüsselwiederherstellung	Backup-Prozesse, -Verfahren und -Techniken zur Bewertung von Betriebskontinuitätsrisiken werden definiert, implementiert und bewertet.

6.21	Schlüssel Bestandsmanagement	Die Prozesse, Verfahren und technischen Maßnahmen des Schlüsselverwaltungssystems werden definiert, implementiert und evaluiert, um alle kryptografischen Materialien und Statusänderungen zu verfolgen und zu melden, einschließlich der gesetzlichen und behördlichen Bestimmungen.
6.22	Verschlüsselung der Übertragung	Verschlüsselung bei der Online-Übertragung von persönlichen Daten. Verschlüsselung von Videostreams, verschlüsselte Verbindung zur Software-Plattform oculavis SHARE (DTLS 1.2, SRTP, HTTPS, TLS 1.2).
7. Lebenszyklusmanagement für Datensicherheit und Datenschutz		
7.1	Sicherheits- und Datenschutzpolitik und verfahren	Es werden Richtlinien und Verfahren für die Klassifizierung, den Schutz und den Umgang mit Daten während ihres gesamten Lebenszyklus gemäß allen geltenden Gesetzen und Vorschriften, Standards und Risikostufen festgelegt, dokumentiert, genehmigt, kommuniziert, durchgesetzt, bewertet und gepflegt. Interne Datenschutz- und IT-Sicherheitsrichtlinien (auf der Grundlage der ISMS-Norm ISO27001), einschließlich der Verfahren gemäß den geltenden Gesetzen und Vorschriften, werden umgesetzt und regelmäßig (im Allgemeinen jährlich) überprüft und bei Bedarf aktualisiert.
7.2	Sichere Entsorgung	Es werden branchenübliche Methoden zur sicheren Datenentsorgung von Speichermedien angewandt, so dass die Informationen nicht durch forensische Mittel wiederhergestellt werden können.

7.3	Daten-Inventarisierung	Verwendung von Verschlüsselung zur Speicherung persönlicher Daten. Passwörter werden als Salted Hash (SHA-256) gespeichert. Datenbanken und Kundendaten im Dateisystem sind verschlüsselt (AES-256). Backups werden ebenfalls verschlüsselt (AES-256). Regelmäßige interne Audits (in der Regel jährlich), um die Einhaltung der Datenschutz- und IT-Sicherheitsrichtlinien zu überprüfen und zu beurteilen, ob sie geeignet sind, den Schutz personenbezogener Daten zu gewährleisten. Interne Penetrationstests werden vor neuen Releases der Softwareprodukte von oculavis durchgeführt. Die Dokumente der internen Audits sind nicht frei zugänglich, aber gefundene Sicherheitslücken werden in den Release Notes dokumentiert.
7.4	Klassifizierung der Daten	Die Daten werden je nach Art und Sensibilitätsgrad klassifiziert. Alle Mitarbeiter sind über die Datenklassifizierung und das Verfahren zur Handhabung der Daten informiert.
7.5	Dokumentation des Datenflusses	Es wird eine Datenflussdokumentation erstellt, aus der hervorgeht, welche Daten verarbeitet werden und wo sie gespeichert und übermittelt werden. Die Dokumentation wird in festgelegten Abständen, mindestens aber jährlich und nach jeder Änderung überprüft.
7.6	Dateneigentum und -verantwortung	Der Besitz und die Verwaltung aller relevanten personenbezogenen und sensiblen Daten wird in einem Bestandsverzeichnis dokumentiert und mindestens einmal jährlich überprüft.
7.7	Datenschutz durch Design und Standard	Systeme, Produkte und Geschäftspraktiken beruhen auf Sicherheitsgrundsätzen und bewährten Verfahren der Branche.
7.8	Datenschutz durch Design und Standard	Für die Umsetzung, Überwachung und Beratung von Datenschutzthemen hat oculavis einen Datenschutzbeauftragten bestellt.

7.9	Datenschutz-Folgenabschätzung	Bei der Verarbeitung personenbezogener Daten wird eine Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) durchgeführt und die Herkunft, Art, Besonderheit und Schwere der Risiken gemäß den geltenden Gesetzen, Vorschriften und bewährten Verfahren der Branche bewertet. Prozesse, Verfahren und technische Maßnahmen werden definiert, implementiert und evaluiert, um sicherzustellen, dass jede Übertragung von personenbezogenen oder sensiblen Daten vor unbefugtem Zugriff geschützt ist und nur im Rahmen des zulässigen Umfangs (gemäß den jeweiligen Gesetzen und Vorschriften) verarbeitet wird.
7.10	Übertragung sensibler Daten	Es werden Prozesse, Verfahren und technische Maßnahmen definiert, umgesetzt und bewertet, die es betroffenen Personen ermöglichen, Zugang zu personenbezogenen Daten zu beantragen, sie zu ändern oder zu löschen (gemäß DSGVO). Es werden Prozesse, Verfahren und technische Maßnahmen festgelegt, umgesetzt und bewertet, um sicherzustellen, dass personenbezogene Daten (gemäß den geltenden Gesetzen und Vorschriften und für die der betroffenen Person erklärten Zwecke) verarbeitet werden.

7.11	Zugang zu personenbezogenen Daten, Widerruf, Berichtigung und Löschung	Es werden Prozesse, Verfahren und technische Maßnahmen für die Übermittlung und Unterverarbeitung personenbezogener Daten festgelegt, umgesetzt und bewertet (gemäß den Bestimmungen der DSGVO). Es werden Prozesse, Verfahren und technische Maßnahmen definiert, implementiert und bewertet, um den Dateneigentümer über jeden Zugriff auf personenbezogene oder sensible Daten durch Unterauftragsverarbeiter vor Beginn der Verarbeitung zu informieren. Der Zugriff auf personenbezogene (Kunden)Daten durch oculavis-Mitarbeiter unterliegt entsprechenden Geheimhaltungsverpflichtungen (Arbeitsvertrag und Vertraulichkeitsvereinbarung, insbesondere im Umgang mit Kundendaten). oculavis speichert personenbezogene Daten nur zur Abwicklung des Geschäftsbetriebes. Der Zugriff auf Kundendaten erfolgt nach Einwilligung des Kunden und nach dem Vier-Augen-Prinzip. Es ist ein Löschkonzept implementiert, das Aufbewahrungsfristen für personenbezogene Daten garantiert. Eine automatische oder halbautomatische Löschung von personenbezogenen Daten findet während der Vertragslaufzeit nicht statt. Bei Vertragsende wird dem Kunden die Möglichkeit gegeben, die Daten aus seiner Software-Plattform oculavis SHARE zu speichern. Alle personenbezogenen Daten werden nach Ablauf der Aufbewahrungsfrist (in der Regel 90 Tage) oder auf Wunsch des Kunden kontrolliert gelöscht und/oder vernichtet. Logdateien werden nach 30 Tagen gelöscht.
7.12	Einschränkung des Zwecks der Verarbeitung personenbezogener Daten	Vor der Replikation oder Verwendung von Produktionsdaten in Nicht-Produktionsumgebungen wird die Genehmigung der Dateneigentümer eingeholt und das damit verbundene Risiko verwaltet. Die Praktiken zur Aufbewahrung, Archivierung und Löschung von Daten entsprechen den geschäftlichen Anforderungen, den geltenden Gesetzen und Vorschriften.
7.13	Personenbezogene Daten - Unterverarbeitungen	Es werden Prozesse, Verfahren und technische Maßnahmen für die Übermittlung und Unterverarbeitung personenbezogener Daten definiert, umgesetzt und bewertet (gemäß DSGVO).

7.14	Offenlegung der Daten von Unterauftragsverarbeitern	Es werden Prozesse, Verfahren und technische Maßnahmen festgelegt, umgesetzt und bewertet, um dem Dateneigentümer vor Beginn der Verarbeitung Einzelheiten über den Zugriff auf personenbezogene oder sensible Daten durch Unterauftragsverarbeiter mitzuteilen.
7.15	Einschränkung der Verwendung von Produktionsdaten	Vor der Replikation oder Verwendung von Produktionsdaten in Nicht-Produktionsumgebungen wird die Genehmigung der Dateneigentümer eingeholt und das damit verbundene Risiko verwaltet.
7.16	Schutz sensibler Daten	Es werden Prozesse, Verfahren und technische Maßnahmen definiert und umgesetzt, um sensible Daten während ihres gesamten Lebenszyklus gemäß der DSGVO zu schützen.
7.17	Benachrichtigung über die Offenlegung	Die Cloud-Service-Provider von oculavis beschreiben oculavis das Verfahren zur Verwaltung und Beantwortung von Anfragen zur Offenlegung personenbezogener Daten durch Strafverfolgungsbehörden gemäß den geltenden Gesetzen und Vorschriften.
7.18	Daten Standort	Es werden Prozesse, Verfahren und technische Maßnahmen definiert und implementiert, um die physischen Datenstandorte festzulegen und zu dokumentieren, einschließlich der Orte, an denen Daten verarbeitet oder gesichert werden.
8. Governance, Risiko und Compliance		
8.1	Richtlinien und Verfahren des Governance-Programms	Die Richtlinien und Verfahren des Information-Governance-Programms, die von der Unternehmensleitung unterstützt werden, werden festgelegt, dokumentiert, genehmigt, kommuniziert, angewendet, bewertet, gepflegt und mindestens jährlich aktualisiert.
8.2	Programm zur Risikoverwaltung	oculavis verfügt über ein formelles, dokumentiertes und von der Unternehmensleitung unterstütztes Risikomanagementprogramm (ERM), das Richtlinien und Verfahren zur Identifizierung, Bewertung, Verantwortlichkeit, Behandlung und Akzeptanz von Sicherheits- und Datenschutzrisiken in der Cloud umfasst.

8.3	Überprüfung der Organisationspolitik	Es erfolgt eine jährliche Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen sowie eine jährliche Überprüfung der Einhaltung der Datenschutz- und IT-Sicherheitsrichtlinien durch den Datenschutz- und IT-Sicherheitsbeauftragten.
8.4	Verfahren für Ausnahmeregelungen	Ein genehmigter Ausnahmeprozess ist durch das bei oculavis etablierte Governance-Programm vorgeschrieben und wird bei jeder Abweichung von einer festgelegten Richtlinie befolgt.
8.5	Programm für Informationssicherheit	Erstschulung neuer Mitarbeiter in den Bereichen Informationssicherheit durch Workshops zum Thema IT-Sicherheit und Datenschutz.
8.6	Governance Verantwortungsmodell	Rollen und Verantwortlichkeiten für die Planung, Umsetzung, Durchführung, Bewertung und Verbesserung von Governance-Programmen sind definiert und dokumentiert.
8.7	Informationssystem Regulatorisches Mapping	Auf Basis der ISO 27001 werden bei oculavis alle relevanten Normen, Vorschriften, gesetzlichen/vertraglichen und satzungsmäßigen Anforderungen identifiziert und dokumentiert.
8.8	Besondere Interessengruppen	Bei oculavis wird der Kontakt zu Cloud-bezogenen Interessengruppen und anderen relevanten Einrichtungen hergestellt und gepflegt.
9. Personalwesen		
9.1	Grundsätze und Verfahren für Hintergrunduntersuchungen	Richtlinien und Verfahren zur Überprüfung des Hintergrunds aller neuen Mitarbeiter (einschließlich, aber nicht beschränkt auf entfernte Mitarbeiter, Auftragnehmer und Dritte) werden festgelegt, dokumentiert, genehmigt, kommuniziert, angewendet, bewertet und aufrechterhalten. Die Richtlinien und Verfahren zur Überprüfung des Hintergrunds werden unter Berücksichtigung lokaler Gesetze, Vorschriften, ethischer Grundsätze und vertraglicher Auflagen entwickelt und stehen in einem angemessenen Verhältnis zur Datenklassifizierung, auf die zugegriffen werden soll, zu den geschäftlichen Anforderungen und zum akzeptablen Risiko. Die Grundsätze und Verfahren zur Überprüfung des Hintergrunds werden mindestens einmal jährlich überprüft und aktualisiert.

9.2	Richtlinien und Verfahren zur akzeptablen Nutzung von Technologie	Richtlinien und Verfahren zur Festlegung von Erlaubnissen und Bedingungen für die zulässige Nutzung von organisatorisch oder verwalteten Vermögenswerten werden festgelegt, dokumentiert, genehmigt, mitgeteilt, angewendet, bewertet, aufrechterhalten und mindestens jährlich aktualisiert.
9.3	Clean-Desk-Politik und -Verfahren	Richtlinien und Verfahren, die vorschreiben, dass unbeaufsichtigte Arbeitsbereiche vertrauliche Daten verbergen müssen, werden festgelegt, dokumentiert, genehmigt, mitgeteilt, angewendet, bewertet, aufrechterhalten und mindestens einmal jährlich aktualisiert.
9.4	Grundsätze und Verfahren für Fern- und Heimarbeit	Richtlinien und Verfahren zum Schutz von Informationen, auf die an entfernten Standorten zugegriffen wird, die dort verarbeitet oder gespeichert werden, werden festgelegt, dokumentiert, genehmigt, weitergegeben, angewendet, bewertet, gepflegt und mindestens einmal jährlich aktualisiert.
9.5	Vermögenserträge	Verfahren zur Rückgabe von Vermögenswerten, die sich im Eigentum der Organisation befinden, durch ausgeschiedene Mitarbeiter sind festgelegt und dokumentiert.
9.6	Vertragsunterlagen	Vertragliche Verpflichtungen (Vertraulichkeitserklärung) im Umgang mit Kundendaten für alle oculavis-Mitarbeiter.
9.7	Beendigung des Arbeitsverhältnisses	Verfahren, die die Aufgaben und Zuständigkeiten im Zusammenhang mit Veränderungen im Beschäftigungsverhältnis beschreiben, werden festgelegt, dokumentiert und dem gesamten Personal mitgeteilt.
9.8	Prozess der Beschäftigungsvereinbarung	Die Mitarbeiter müssen eine Arbeitsvereinbarung unterzeichnen, bevor sie Zugang zu den Informationssystemen, Ressourcen und Vermögenswerten der Organisation erhalten.
9.9	Inhalt der Arbeitsvereinbarung	In den Arbeitsverträgen sind Bestimmungen und/oder Bedingungen für die Einhaltung der festgelegten Richtlinien zur Informationsverwaltung und -sicherheit enthalten.
9.10	Rollen und Zuständigkeiten des Personals	Die Aufgaben und Zuständigkeiten der Mitarbeiter in Bezug auf Informationswerte und -sicherheit sind dokumentiert und werden kommuniziert.

9.11	Vertraulichkeitsvereinbarungen	Anforderungen an Geheimhaltungs-/Vertraulichkeitsvereinbarungen, die den organisatorischen Datenschutzbedarf und betriebliche Details widerspiegeln, werden ermittelt, dokumentiert und in geplanten Abständen überprüft.
9.12	Schulung zum Sicherheitsbewusstsein	Regelmäßige Schulung der Mitarbeiter in den Bereichen Datenschutz und IT-Sicherheit durch zweiwöchentliche Betriebsversammlungen zum Thema IT-Sicherheit und Datenschutz.
9.13	Compliance Verantwortung der Benutzer	Die Mitarbeiter werden über ihre Aufgaben und Verantwortlichkeiten informiert, um das Bewusstsein für und die Einhaltung von festgelegten Richtlinien, Verfahren und geltenden rechtlichen, gesetzlichen oder behördlichen Verpflichtungen aufrechtzuerhalten.
10. Identitäts- und Zugangsmanagement		
10.1	Richtlinien und Verfahren für das Identitäts- und Zugangsmanagement	Der Zugriff auf personenbezogene (Kunden)Daten durch oculavis-Mitarbeiter unterliegt entsprechenden Geheimhaltungsverpflichtungen (Arbeitsvertrag und Vertraulichkeitsvereinbarung, insbesondere über den Umgang mit Kundendaten).
10.2	Starke Passwort-Richtlinie und -Verfahren	Es werden strenge Passwortrichtlinien und -verfahren festgelegt, dokumentiert, genehmigt, mitgeteilt, umgesetzt, angewendet, bewertet und mindestens einmal jährlich aktualisiert.
10.3	Identitätsinventar	Systemidentitätsinformationen und Zugriffsebenen werden verwaltet, gespeichert und überprüft.
10.4	Trennung der Zuständigkeiten	Bei der Umsetzung des Zugangs zu Informationssystemen wird der Grundsatz der Aufgabentrennung angewandt.
10.5	Geringstes Privileg	Die Vergabe von Berechtigungen und Zugängen erfolgt nach dem Need-to-know-Prinzip unter Berücksichtigung der Sensibilität und Kritikalität der Datenverarbeitung sowie der Verantwortung des Mitarbeiters im Unternehmen. Die Vergabe und Gewährung von Berechtigungen und Zugängen erfolgt nach dem Need-to-know-Prinzip unter Berücksichtigung der Sensibilität und Kritikalität der Datenverarbeitung und der Verantwortlichkeiten des Mitarbeiters im Unternehmen.

10.6	Bereitstellung von Benutzerzugängen	Es wird ein Prozess für die Bereitstellung des Benutzerzugriffs definiert und implementiert, der Änderungen des Daten- und Asset-Zugriffs autorisiert, aufzeichnet und kommuniziert.
10.7	Änderungen und Entzug des Benutzerzugangs	Es gibt ein Verfahren zur rechtzeitigen Aufhebung oder Änderung des Zugriffs von Personen, die umziehen oder ausscheiden, oder zur Änderung der Systemidentität, um Identitäts- und Zugriffsverwaltungsrichtlinien wirksam einzuführen und zu vermitteln.
10.8	Überprüfung des Benutzerzugangs	Die Überprüfung und Neubewertung des Benutzerzugriffs im Hinblick auf die geringsten Rechte und die Aufgabentrennung erfolgt mit einer Häufigkeit, die der Risikotoleranz des Unternehmens entspricht.
10.9	Trennung von Rollen mit privilegiertem Zugriff	Prozesse, Verfahren und technische Maßnahmen für die Trennung privilegierter Zugriffsrollen sind so definiert, implementiert und evaluiert, dass der administrative Datenzugriff, die Verschlüsselung, die Schlüsselverwaltung und die Protokollierung getrennt sind.
10.10	Verwaltung von Rollen mit privilegiertem Zugriff	Ein Zugriffsprozess wird definiert und implementiert, um sicherzustellen, dass privilegierte Zugriffsrollen und -rechte für einen begrenzten Zeitraum gewährt werden. Es werden Verfahren implementiert, um die Ausweitung des privilegierten Zugriffs zu verhindern.
10.11	Wahrung der Integrität von Protokollen	Prozesse, Verfahren und technische Maßnahmen, die sicherstellen, dass die Protokollierungsinfrastruktur für alle (einschließlich privilegierter Zugriffsrollen) „schreibgeschützt“ ist, werden definiert, umgesetzt und bewertet. Die Möglichkeit, die „Nur-Lesen“-Konfiguration der Protokollierungsinfrastruktur zu deaktivieren, wird durch ein Verfahren kontrolliert, das die Aufgabentrennung gewährleistet.
10.12	Eindeutig identifizierbare Benutzer	Prozesse, Verfahren und technische Maßnahmen, die sicherstellen, dass Benutzer durch eine eindeutige Identifizierung identifizierbar sind (oder Personen mit der Verwendung der Benutzeridentifikation in Verbindung gebracht werden können), werden definiert, umgesetzt und bewertet.

10.13	Starke Authentifizierung	Prozesse, Verfahren und technische Maßnahmen für die Authentifizierung des Zugangs zu Systemen, Anwendungen und Datenbeständen, einschließlich der Multifaktor-Authentifizierung für einen am wenigsten privilegierten Benutzer und den Zugang zu sensiblen Daten, werden definiert, umgesetzt und bewertet. Digitale Zertifikate oder Alternativen, die ein gleichwertiges Sicherheitsniveau für Systemidentitäten erreichen, werden eingeführt.
10.14	Verwaltung von Passwörtern	Prozesse, Verfahren und technische Maßnahmen für die sichere Verwaltung von Passwörtern werden definiert, implementiert und bewertet.
10.15	Autorisierungsmechanismen	Prozesse, Verfahren und technische Maßnahmen zur Überprüfung des Zugriffs auf Daten und Systemfunktionen sind autorisiert, definiert, implementiert und bewertet.
11. Sicherheit von Infrastruktur und Virtualisierung		
11.1	Kapazitäts- und Ressourcenplanung	Verfügbarkeit, Qualität und Kapazität der Ressourcen werden so geplant und überwacht, dass die vom Unternehmen geforderte Systemleistung erbracht wird.
11.2	Netzwerksicherheit	Die Kommunikation zwischen den Umgebungen wird überwacht und verschlüsselt. Der Schutz des internen Netzes vor unbefugtem Zugriff wird durch ein Sicherheitsgateway mit Firewall und IDS-Modul gewährleistet. Die Netzwerkkonfigurationen werden mindestens einmal jährlich überprüft und durch eine dokumentierte Begründung aller erlaubten Dienste, Protokolle, Ports und kompensierenden Kontrollen unterstützt.
11.3	Produktions- und Nicht-Produktionsumgebungen	Die Softwareplattform für den Kunden läuft auf einer eigenen Kundeninstanz und ist vollständig von anderen Kundeninstanzen isoliert. Darüber hinaus wird die Plattform in Module aufgeteilt und nach dem Docker-Konzept (Sandbox-Konzept) bereitgestellt, so dass die einzelnen Module (Datenbank, Frontend, Backend) zusätzlich isoliert sind.

11.4	Segmentierung und Segregation	Strikte Trennung von Test- /Entwicklungsdaten/-plattformen und Produktionsdaten/-plattformen. Nur die Administratorengruppe der Software hat Zugriff auf die Kundeninstanzen (Produktionsumgebung) und das auch nur für Backup-, Update- oder Datenwiederherstellungszwecke. Anomalien im Zugriff werden durch das Incident Management von oculavis bearbeitet.
11.5	Migration zu Cloud-Umgebungen	oculavis hat sichere und verschlüsselte Kommunikationskanäle implementiert. Bei der Migration von Servern, Diensten, Anwendungen oder Daten in Cloud-Umgebungen werden ausschließlich aktuelle und genehmigte Protokolle verwendet.
11.6	Dokumentation der Netzwerkarchitektur	Identifizierung und Dokumentation risikoreicher Umgebungen.
11.7	Netzwerk-Verteidigung	Es werden Prozesse, Verfahren und Abwehrtechniken zum Schutz, zur Erkennung und zur rechtzeitigen Reaktion auf netzbasierte Angriffe definiert, implementiert und bewertet.
11.8	Vermögensverwaltung	Die mit den Informationen und den Einrichtungen zur Informationsverarbeitung verbundenen Vermögenswerte werden ermittelt, und es wird ein Inventar dieser Vermögenswerte mit klaren Zuständigkeiten erstellt und regelmäßig (im Allgemeinen jährlich) gepflegt. Alle Informationen werden in Bezug auf rechtliche Anforderungen, Wert, Kritikalität und Empfindlichkeit gegenüber unbefugter Offenlegung oder Änderung klassifiziert. Eine Reihe von Verfahren zur Kennzeichnung und Handhabung von Informationen wird entsprechend dem Informationsklassifizierungsschema umgesetzt.
11.9	Sicherheits-Gateway	Der Schutz des internen Netzwerks vor unbefugten Zugriffen wird durch ein Sicherheitsgateway mit Firewall und IDS-Modul gewährleistet.

12. Protokollierung und Überwachung

12.1	Grundsätze und Verfahren für die Protokollierung und Überwachung	Strategien und Verfahren für die Protokollierung und Überwachung werden festgelegt, dokumentiert, genehmigt, mitgeteilt, angewendet, bewertet, aufrechterhalten und mindestens einmal jährlich aktualisiert. Es findet eine pseudonymisierte Protokollierung aller Datenzugriffe mit Zeitstempel auf Instanzen des Clients statt. Die Protokolldateien können nur von Administratoren eingesehen werden und sind gegen unbefugte Manipulationen geschützt. Die Vergabe von Berechtigungen wird detailliert mit vollem Namen dokumentiert. Der Datenschutzbeauftragte überwacht die Zugriffe der berechtigten Personen auf Instanzen des Clients. Logdateien im Hintergrund der Software dokumentieren Systemanpassungen und dienen dazu, Fehlerzustände zu vermeiden, mögliche Angriffe auf das System zu erkennen und die Nachvollziehbarkeit von Systemaktivitäten zu gewährleisten.
12.2	Schutz von Audit-Protokollen	Es werden Prozesse, Verfahren und technische Maßnahmen definiert, implementiert und evaluiert, um die Sicherheit und Aufbewahrung von Audit-Logs zu gewährleisten. Der Datenschutzbeauftragte überwacht die Zugriffe der berechtigten Personen auf Instanzen des Mandanten.
12.3	Sicherheitsüberwachung und Alarmierung	Sicherheitsrelevante Ereignisse werden innerhalb von Anwendungen und der zugrunde liegenden Infrastruktur ermittelt und überwacht. Es wird ein Prozess definiert und implementiert, um auf der Grundlage von sicherheitsrelevanten Ereignissen und den entsprechenden Metriken Warnungen an die verantwortlichen Akteure zu übermitteln.
12.4	Prüfungsprotokolle Zugang und Rechenschaftspflicht	Der Zugang zu den Prüfprotokollen ist auf autorisiertes Personal beschränkt, und es werden Aufzeichnungen geführt, um eine eindeutige Zugriffsverantwortung zu gewährleisten.
12.5	Audit-Protokolle Überwachung und Reaktion	Sicherheitsauditprotokolle werden überwacht, um Aktivitäten zu erkennen, die von typischen oder erwarteten Mustern abweichen. Es wird ein Verfahren eingeführt und befolgt, um festgestellte Anomalien zu überprüfen und rechtzeitig geeignete Maßnahmen zu ergreifen.

12.6	Synchronisierung der Uhr	In allen relevanten Informationsverarbeitungssystemen wird eine verlässliche Zeitquelle verwendet.
12.7	Log-Schutz	Das Informationssystem schützt die Protokolle vor unberechtigtem Zugriff, Änderung und Löschung.
12.8	Protokolle der Zugangskontrolle	Der physische Zugang wird protokolliert und durch ein auditierbares Zugangskontrollsystem überwacht.
12.9	Meldung von Fehlern und Anomalien	Verfahren und technische Maßnahmen zur Meldung von Anomalien und Ausfällen des Überwachungssystems sind definiert, umgesetzt und bewertet. Verantwortliche werden unverzüglich über Anomalien und Ausfälle informiert.
13. Management von Sicherheitsvorfällen, E-Discovery und Cloud-Forensik		
13.1	Politik und Verfahren für das Management von Sicherheitsvorfällen	Richtlinien und Verfahren für das Management von Sicherheitsvorfällen, E-Discovery und Cloud-Forensik werden festgelegt, dokumentiert, genehmigt, kommuniziert, angewendet, bewertet, gepflegt, überprüft und jährlich aktualisiert.
13.2	Politik und Verfahren für das Dienstleistungsmanagement	Richtlinien und Verfahren für die rechtzeitige Bewältigung von Sicherheitsvorfällen werden festgelegt, dokumentiert, genehmigt, mitgeteilt, angewandt, bewertet, aufrechterhalten, überprüft und mindestens einmal jährlich aktualisiert.
13.3	Pläne für die Reaktion auf Zwischenfälle	Es gibt einen Notfallplan, wie im Falle eines Vorfalls sofort gehandelt werden kann. Nachdem ein Sicherheits-/Datenschutzvorfall identifiziert wurde, erfolgt eine Dokumentation, Analyse und Bewertung des Sicherheits-/Datenschutzvorfalls. Anschließend werden Maßnahmen ergriffen und im Falle eines kundenrelevanten Vorfalls wird der Kunde innerhalb von 24 Stunden per E-Mail/Telefon über den Vorfall und die Maßnahmen informiert.
13.4	Tests zur Reaktion auf Zwischenfälle	Der Plan für die Reaktion auf Sicherheitsvorfälle wird in geplanten Abständen oder bei wesentlichen organisatorischen oder umgebungsbedingten Änderungen auf seine Wirksamkeit geprüft und gegebenenfalls aktualisiert.

13.5	Metriken zur Reaktion auf Vorfälle	Metriken für Informationssicherheitsvorfälle werden erstellt und überwacht.
13.6	Benachrichtigung bei Sicherheitsverletzungen	Prozesse, Verfahren und technische Maßnahmen für die Meldung von Sicherheitsverletzungen werden festgelegt und umgesetzt. Sicherheitsverstöße und vermutete Sicherheitsverstöße werden gemeldet (einschließlich relevanter Verstöße in der Lieferkette).
13.7	Kontaktstellen Wartung	Es gibt Kontaktstellen für die zuständigen Regulierungsbehörden, die nationalen und lokalen Strafverfolgungsbehörden und andere Behörden, die der Rechtsprechung unterliegen.
14. Management der Lieferkette, Transparenz und Rechenschaftspflicht		
14.1	SSRM-Politik und -Verfahren	Richtlinien und Verfahren zur Umsetzung des Modells der geteilten Sicherheitsverantwortung (SSRM) innerhalb der Organisation werden festgelegt, dokumentiert, genehmigt, kommuniziert, angewandt, bewertet, aufrechterhalten, überprüft und jährlich aktualisiert.
14.2	Risikomanagement in der Lieferkette	Risikofaktoren werden mit allen Organisationen innerhalb der Lieferkette in Verbindung gebracht und von oculavis regelmäßig überprüft.
14.3	Primärdienst und vertragliche Vereinbarung	Servicevereinbarungen zwischen oculavis und Kunden (Mietern) enthalten mindestens die folgenden einvernehmlich vereinbarten Bestimmungen und/oder Bedingungen: • Umfang, Merkmale und Ort der Geschäftsbeziehung und der angebotenen Dienstleistungen • Anforderungen an die Informationstechnologie • Protokollierungs- und Überwachungsmöglichkeiten • Verfahren für das Management von Vorfällen und die Kommunikation • Recht auf Prüfung und Bewertung durch Dritte • Beendigung der Dienstleistung

		• Anforderungen an Interoperabilität und Übertragbarkeit • Datenschutz
14.4	Interne Konformitätsprüfung	Auf der Grundlage von ISO 27001 gibt es ein Verfahren zur mindestens jährlichen Durchführung interner Bewertungen, um die Konformität und Wirksamkeit von Standards, Richtlinien, Verfahren und SLA-Aktivitäten zu bestätigen.
14.5	Bewertung der Datensicherheit in der Lieferkette	Ein Verfahren zur Durchführung von Sicherheitsbewertungen für alle Unternehmen der Lieferkette wird definiert und umgesetzt.
14.6	Unterauftragnehmer	Für die Auswahl von Unterauftragnehmern gibt es einen klaren Prozess. Mit den von der oculavis GmbH beauftragten Unterauftragnehmern sind formalisierte, dokumentierte und kontrollierte Datenverarbeitungsverträge abgeschlossen und alle Unterauftragsverarbeiter werden regelmäßig kontrolliert. Datenschutzkonforme Datenverarbeitungsverträge mit Unterauftragnehmern durch abgeschlossene EU-Standardvertragsklauseln.
14.7	Zuständigkeiten	Klare Unterscheidung zwischen den Verantwortungsbereichen des Auftraggebers und des Auftragnehmers.
14.8	Beschaffungsprozess	Die Beschaffung von Hardware und Software ist zentralisiert. Alle Beschaffungen werden inventarisiert.
15. Management von Bedrohungen und Schwachstellen		
15.1	Richtlinien und Verfahren zum Management von Bedrohungen und Schwachstellen	Richtlinien und Verfahren werden erstellt, dokumentiert, genehmigt, kommuniziert, angewandt, bewertet und aufrechterhalten, um Schwachstellen zu identifizieren, zu melden und nach Prioritäten zu ordnen, um Systeme vor der Ausnutzung von Schwachstellen zu schützen. Die Richtlinien und Verfahren für das Bedrohungs- und Schwachstellenmanagement werden mindestens einmal jährlich überprüft und aktualisiert.

15.2	Richtlinien und Verfahren zum Schutz vor Malware	Richtlinien und Verfahren zum Schutz vor Malware auf verwalteten Vermögenswerten werden festgelegt, dokumentiert, genehmigt, kommuniziert, angewandt, bewertet, aufrechterhalten, überprüft und mindestens einmal jährlich aktualisiert.
15.3	Zeitplan für die Behebung von Schwachstellen	Prozesse, Verfahren und technische Maßnahmen werden definiert, implementiert und evaluiert, um planmäßige und Notfallreaktionen auf erkannte Schwachstellen zu ermöglichen (basierend auf dem identifizierten Risiko).
15.4	Updates zur Erkennung	Es werden Prozesse, Verfahren und technische Maßnahmen definiert, implementiert und evaluiert, um Erkennungstools, Bedrohungssignaturen und Kompromissindikatoren regelmäßig zu aktualisieren.
15.5	Schwachstellen in externen Bibliotheken	Es werden Prozesse, Verfahren und technische Maßnahmen definiert, implementiert und evaluiert, um Updates für Anwendungen zu identifizieren, die Drittanbieter- oder Open-Source-Bibliotheken verwenden (gemäß der oculavis-Richtlinie zum Schwachstellenmanagement).
15.6	Penetrationstests	Interne Penetrationstests werden vor neuen Releases der Softwareprodukte von oculavis durchgeführt. Die Dokumente der internen Prüfungen sind nicht frei zugänglich, aber die gefundenen Schwachstellen werden in den Release Notes dokumentiert.
15.7	Identifizierung von Schwachstellen	Mindestens monatlich werden Prozesse, Verfahren und technische Maßnahmen zur Erkennung von Schwachstellen in den von der Organisation verwalteten Anlagen festgelegt, umgesetzt und bewertet.
15.8	Priorisierung von Schwachstellen	Die Behebung von Schwachstellen wird anhand eines risikobasierten Modells aus einem branchenweit anerkannten Rahmenwerk nach Prioritäten geordnet.
15.9	Schwachstellenmanagement-Berichterstattung	Es wird ein Prozess definiert und implementiert, um die Identifizierung von Schwachstellen und die Behebung von Schwachstellen zu verfolgen und zu melden, einschließlich der Benachrichtigung der Beteiligten.

15.10	Metriken für das Schwachstellenmanagement	Es werden Metriken für die Identifizierung und Behebung von Schwachstellen festgelegt, überwacht und in bestimmten Abständen berichtet.
16. Universelle Endpunktverwaltung		
16.1	Richtlinie und Verfahren für Endpunktgeräte	Richtlinien und Verfahren werden für alle Endpunkte erstellt, dokumentiert, genehmigt, kommuniziert, angewendet, bewertet und gepflegt. Die Richtlinien und Verfahren für die universelle Endpunktverwaltung werden mindestens einmal jährlich überprüft und aktualisiert.
16.2	Antrag und Dienstgenehmigung	Es gibt eine definierte, dokumentierte, anwendbare und bewertete Liste mit genehmigten Diensten, Anwendungen und den Quellen von Anwendungen (Speichern), die von Endgeräten für den Zugriff auf oder die Speicherung von vom Unternehmen verwalteten Daten verwendet werden dürfen.
16.3	Kompatibilität	Es wird ein Prozess definiert und implementiert, um die Kompatibilität von Endgeräten mit Betriebssystemen und Anwendungen zu überprüfen.
16.4	Endpunkt-Inventarisierung	Ein Inventar aller Endgeräte, die zur Speicherung von und zum Zugriff auf Unternehmensdaten verwendet werden, wird gepflegt.
16.5	Endpunkt-Management	Prozesse, Verfahren und technische Maßnahmen werden definiert, implementiert und evaluiert, um Richtlinien und Kontrollen für alle Endgeräte durchzusetzen, die auf Systeme zugreifen und/oder Unternehmensdaten speichern, übertragen oder verarbeiten dürfen.
16.6	Automatischer Sperrbildschirm	Alle relevanten Endpunkte für die interaktive Nutzung sind so konfiguriert, dass sie einen automatischen passwortgeschützten Sperrbildschirm erfordern.

16.7	Betriebssysteme	Änderungen an Endpunkt-Betriebssystemen, Patch-Levels und/oder Anwendungen werden über den organisatorischen Änderungsmanagementprozess verwaltet.
16.8	Verschlüsselung der Speicherung	Informationen werden auf verwalteten Endgeräten durch Speicherverschlüsselung vor unbefugter Offenlegung geschützt.
16.9	Anti-Malware-Erkennung und -Prävention	Basierend auf dem von oculavis benötigten Risikomanagement werden Malware-Erkennungs- und Präventionsdienste auf den verwalteten Endgeräten konfiguriert.
16.10	Software-Firewall	Software-Firewalls werden auf verwalteten Endpunkten konfiguriert.
16.11	Prävention von Datenverlusten	Verwaltete Endgeräte werden mit Technologien zur Verhinderung von Datenverlusten (DLP) konfiguriert, und die Regeln werden auf der Grundlage einer Risikobewertung definiert.
16.12	Fernortung	Remote-Geolokalisierungsfunktionen sind für alle verwalteten mobilen Endgeräte aktiviert.
16.13	Fernwischen	Es werden Prozesse, Verfahren und technische Maßnahmen definiert, implementiert und evaluiert, um die Fernlöschung von Unternehmensdaten auf verwalteten Endgeräten zu ermöglichen.
16.14	Sicherheitsposition für Endgeräte von Drittanbietern	Prozesse, Verfahren und technische und/oder vertragliche Maßnahmen werden definiert, implementiert und evaluiert, um die Sicherheit von Endgeräten Dritter mit Zugang zu Unternehmensressourcen zu gewährleisten.
17. Software-Produkt		
17.1	Software-Release-Prozess	Für die Softwareversionen von oculavis SHARE gibt es ein formales Freigabeverfahren, wobei die Anforderungen an den Datenschutz und die IT-Sicherheit Teil des Software-Release-Prozesses sind. Die Releases werden alle 6-8 Wochen ausgeliefert.

17.2	Lizenzverwaltung	Keine Installation von Fremdsoftware ohne Lizenzrechte. Für oculavis SHARE wird eine Liste der Bibliotheken/Abhängigkeiten mit deren Lizenzinformationen geführt und regelmäßig überprüft/aktualisiert (Teil des Software-Release-Prozesses).
17.3	Patch-Verwaltung	Aktualisierung der gesamten im Zusammenhang mit der Datenverarbeitung eingesetzten Software und IT (z.B. durch Updates, Patches, Fixes etc.). Bei der oculavis GmbH existiert ein Patch- und Schwachstellenmanagement, insbesondere ein Monitoring für verfügbare (Sicherheits-)Patches der relevanten eingesetzten Bibliotheken/Systeme. Patches werden zeitnah eingespielt und die Bibliotheken auf dem neuesten Stand gehalten. In der Regel werden Patches für oculavis SHARE alle 6-8 Wochen ausgeliefert. Je nach Schweregrad und BSI-Empfehlung können Sicherheitslücken auch früher behoben und als „Hot Fixes“ eingespielt werden (typischerweise innerhalb von vier Wochen nach Veröffentlichung eines Updates/einer Schwachstelle).
17.4	Änderungsmanagement	Bei der oculavis GmbH existiert ein formaler Change Management Prozess, insbesondere im Bereich der Softwareentwicklung und -bereitstellung (Kundeninstanzen). Änderungswünsche werden über den Product Owner formell in das Backlog eingetragen. Es folgt eine Prioritätsbewertung, eine technische Einordnung und Sicherheitsbewertung der Änderung sowie eine grobe Zeitabschätzung. Umgesetzte Änderungen werden innerhalb von Sprints entwickelt/umgesetzt und intensiv getestet, und es gibt einen formalen Überprüfungsprozess, insbesondere für sicherheitsrelevante Änderungen.
17.5	Fernunterstützung	Es wurden Richtlinien für die Fernwartung und den Support eingeführt.
17.6	Sicheres Scrum	IT-Sicherheit ist Teil des agilen Entwicklungsprozesses der Software oculavis SHARE nach dem 4-Phasen-Modell: • Planung und Analyse (Backlog) • Sichere Implementierung • Verifikation und Sicherheitstests • Security-Gate als Teil des DoD

17.7	oculavis SHARE-Administratoren	oculavis SHARE-Administratoren werden regelmäßig darin geschult, wie sie vertrauliche Authentifikatoren (Passwörter, Schlüssel usw.) verwenden, wie sie den besonderen Zugang nutzen und wie sie ihrer besonderen Rolle und Verantwortung gerecht werden.
17.8	Sichere Kodierung	Regelmäßige (bei Stellenantritt und dann mindestens jährlich) Schulungen zu Secure Scrum Development und Secure Coding auf Basis der OWASP-Empfehlungen für alle Softwareentwickler von oculavis SHARE.
17.9	Regelmäßige Überprüfung	Regelmäßige Überprüfung, Beurteilung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen sowie regelmäßige Überprüfung der Einhaltung der Datenschutz- und IT-Sicherheitsrichtlinien durch den Datenschutz- und IT-Sicherheitsbeauftragten.
17.10	Überprüfung der Eingaben	Benutzereingaben werden streng validiert, um Injektionsangriffe (z. B. SQL-Injektionen oder XSS) zu verhindern.
17.11	Protokollierung	Es findet eine pseudonymisierte Protokollierung aller Datenzugriffe mit Zeitstempel auf Instanzen des Clients statt. Die Protokolldateien können nur von Administratoren eingesehen werden und sind gegen unbefugte Manipulationen geschützt. Die Vergabe von Berechtigungen wird detailliert mit vollem Namen dokumentiert. Der Datenschutzbeauftragte überwacht die Zugriffe der berechtigten Personen auf Instanzen des Clients. Logdateien im Hintergrund der Software dokumentieren Systemanpassungen und dienen dazu, Fehlerzustände zu vermeiden, mögliche Angriffe auf das System zu erkennen und die Nachvollziehbarkeit von Systemaktivitäten zu gewährleisten.
17.12	Überwachung	Die Kundeninstanzen und die IT-Infrastruktur der oculavis GmbH werden überwacht, um Anomalien, mögliche bösartige Aktivitäten oder Serverausfälle zu erkennen.
18. Physische Sicherheit		
18.1	Alarm	Alarmüberwachtes Gebäude, Büroflächen und separat gesicherter Serverraum.

18.2	Sicherheits-Token	Verwendung von persönlichen Sicherheitstoken für den Zugang zum Gebäude und zu den Büroräumen, einschließlich der Protokollierung des Zugangs.
18.3	Zugriffsberechtigungen	oculavis hat physische Zutrittsberechtigungen für Mitarbeiter und Dritte (Besucher, Kunden, Reinigungspersonal, Handwerker etc.) implementiert, einschließlich der Beantragung, Genehmigung und Aufhebung des Zutritts.
18.4	Gesicherter Serverraum	Separates Schlüsselsystem für den Serverraum mit namenscharfer Vergabe von Zugangsberechtigungen und Protokollierung der Zugriffe. Der Zugangsschutz zu den Serverfarmen unserer Hosting-Provider hängt von den physikalischen Sicherheitsmaßnahmen des Hosting-Providers ab.
18.5	Verwaltung von Mediengeräten	Es werden Verfahren für die Verwaltung von Medien/Wechseldatenträgern gemäß dem Klassifizierungsschema eingeführt. Nicht mehr benötigte Datenträger werden unter Anwendung dieser formalen Verfahren sicher entsorgt.
19. Interoperabilität und Portabilität		
19.1	Grundsätze und Verfahren für Interoperabilität und Portabilität	Für die Kommunikation zwischen Anwendungsdiensten (z. B. APIs), die Interoperabilität der Informationsverarbeitung, die Übertragbarkeit der Anwendungsentwicklung, den Informations-/Datenaustausch, die Nutzung, die Übertragbarkeit, die Integrität und die Persistenz werden Richtlinien und Verfahren festgelegt, dokumentiert, genehmigt, mitgeteilt, angewandt, bewertet und gepflegt. Diese Richtlinien und Verfahren werden mindestens einmal jährlich überprüft und aktualisiert.
19.2	Verfügbarkeit der Anwendungsschnittstelle	oculavis kann Daten über eine Anwendungsschnittstelle programmatisch abrufen, um Interoperabilität und Portabilität zu ermöglichen.
19.3	Sichere Interoperabilität und Portabilitätsmanagement	Für die Verwaltung, den Import und den Export von Daten werden kryptografisch sichere und standardisierte Netzwerkprotokolle eingesetzt.