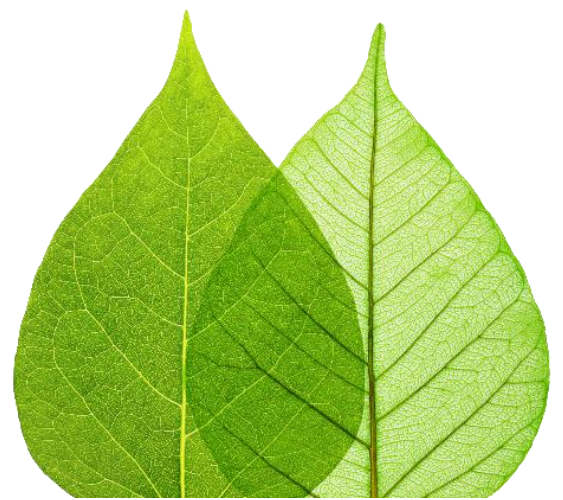




Leitlinie zur Informationssicherheit

synava GmbH und medavis GmbH / Version 2.0



Dokumentenhistorie

Version/Datum	Bearbeitung	Grund der Änderung
2.0 / 01.07.2026	Günter Hellstern	Neuerstellung im Rahmen der Erweiterung des Zertifizierungsgeltungsbereichs auf die synava GmbH; Ablösung der bisherigen, medavis-spezifischen Leitlinie vom 29.01.2020

1. Einordnung

1.1 Auftrag und Geschäftszweck

Die synava GmbH erbringt als zentrale Gesellschaft der Firmengruppe Querschnittsfunktionen für die Mitglieder der synava-Gruppe, insbesondere in den Bereichen IT, Personal (HR), Finanzen, Einkauf, Marketing und Facility Management. Über diese Funktionen trägt die synava GmbH wesentlich zur einheitlichen Steuerung und Absicherung der Informationssicherheit innerhalb der gesamten Gruppe bei.

Die medavis GmbH ist eine Gesellschaft in der synava-Gruppe und entwickelt IT-Systeme für das Gesundheitswesen, insbesondere für niedergelassene Radiologien und Kliniken. Zum Produktportfolio zählen ein Radiologie-Informationssystem, Patienten- und Zuweiserportale, eine Buchungsplattform, eine Teleradiologie-Plattform sowie ein PACS.

Ein Teil dieser Lösungen wird als medizinische Software-as-a-Service (SaaS) in der Cloud betrieben.

Die Kunden der medavis GmbH verarbeiten mit diesen Systemen besonders schutzwürdige Gesundheitsdaten (Art. 9 DSGVO). Ein Teil der Kliniken, die medavis-Produkte einsetzen, unterliegt als Betreiber Kritischer Infrastrukturen (KRITIS) im Sektor Gesundheitswesen besonderen gesetzlichen Anforderungen an die IT-Sicherheit (u. a. § 8a BSIG, § 391 SGB V, branchenspezifischer Sicherheitsstandard B3S). Die medavis GmbH ist als Softwarehersteller und Cloud-Betreiber selbst kein KRITIS-Betreiber, jedoch ein für die Aufgabenerfüllung dieser Einrichtungen wesentlicher Dienstleister. Aus dieser Rolle in der Lieferkette leiten sich Sorgfaltspflichten ab. Darüber hinaus ist die medavis GmbH aufgrund ihrer Fernwartungsleistungen als Anbieter verwalteter Dienste (Managed Service Provider) eine wichtige Einrichtung im Sinne des BSIG in der Fassung des NIS-2-Umsetzungsgesetzes und beim BSI registriert.

Als Hersteller von Produkten mit digitalen Elementen unterliegt sie zudem dem Cyber Resilience Act (CRA).

Kunden, die cloud-basierte SaaS-Produkte einsetzen, fordern vertraglich und regulatorisch ein angemessenes und nachvollziehbares Sicherheitsniveau. Diese Kundenanforderungen bilden einen wesentlichen Maßstab für die Informationssicherheit bei medavis.

Der Erfolg der medavis GmbH beruht wesentlich auf dem Vertrauen der Kunden in die Verfügbarkeit, Integrität und Vertraulichkeit der eingesetzten Systeme. Störungen der Informationssicherheit können unmittelbar die diagnostische und therapeutische Versorgung von Patientinnen und Patienten beeinträchtigen.

1.2 Zweck der Leitlinie

Diese Leitlinie beschreibt die strategischen Ziele und Rahmenbedingungen zur Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit bei der synava GmbH und der medavis GmbH.

Die Geschäftsführung

- betreibt ein Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001:2022 sowie – für die betroffenen Cloud-Produkte – nach dem BSI-Anforderungskatalog Cloud Computing C5,
- stellt eine Informationssicherheitsorganisation mit klar benannten Rollen und Verantwortlichkeiten bereit,
- integriert Informationssicherheit als festen Bestandteil der Produktentwicklung (Secure Software Development Lifecycle), der Aufbau- und Ablauforganisation sowie relevanter Projekte,
- steuert Subdienstleister und Auftragsverarbeiter (z. B. Cloud- und Kommunikationsdienstleister) über geeignete vertragliche und technisch-organisatorische Maßnahmen,
- beauftragt regelmäßige interne und externe Audits zur Überprüfung des erreichten Sicherheitsniveaus,
- stellt die für die Umsetzung notwendigen personellen, sachlichen und finanziellen Ressourcen bereit,
- überprüft diese Leitlinie sowie das ISMS mindestens jährlich oder anlassbezogen bei wesentlichen Änderungen und passt sie bei Bedarf an,
- verpflichtet sich zur kontinuierlichen Verbesserung des Informationssicherheits-Managementsystems und seiner Wirksamkeit.

1.3 Geltungsbereich

Diese Leitlinie gilt gemeinsam und vollständig für die synava GmbH und die medavis GmbH. Im Rahmen der Zertifizierung nach ISO/IEC 27001 fungiert die synava GmbH als Hauptstandort (Zentrale) im Sinne der IAF MD 1; die medavis GmbH gilt als Nebenstandort. Die synava GmbH übt die betriebliche Kontrolle über das gemeinsame ISMS aus,

insbesondere hinsichtlich der Festlegung dieser Leitlinie, der Steuerung des internen Auditprogramms sowie der Durchführung des Management-Reviews für alle einbezogenen Standorte.

Die Leitlinie gilt für alle Standorte, Produkte und Geschäftsprozesse beider Gesellschaften. Ebenso gilt sie für Dienstleistungen, die die synava GmbH für alle Mitglieder der synava-Gruppe erbringt. Sie umfasst neben der Sicherheit von IT-Systemen und den darin verarbeiteten Daten auch die Sicherheit nicht elektronisch verarbeiteter Informationen (z. B. Papierunterlagen, mündliche Kommunikation).

Die Leitlinie gilt verbindlich für alle Mitarbeiterinnen und Mitarbeiter der synava GmbH und der medavis GmbH – einschließlich Führungskräften, Auszubildenden, Praktikantinnen und Praktikanten sowie Werkstudierenden – und für alle Personen und Unternehmen, die im Rahmen von Werk-, Dienst- oder sonstigen Verträgen mit der Verarbeitung von Informationen der synava GmbH, der medavis GmbH oder ihrer Kunden betraut sind, insbesondere Subdienstleister und Auftragsverarbeiter.

2. Bezug zu rechtlichen und regulatorischen Anforderungen

Für die Informationssicherheit bei synava und medavis sind insbesondere die folgenden gesetzlichen, regulatorischen, vertraglichen und normativen Anforderungen und Rahmenwerke maßgeblich:

- Datenschutz-Grundverordnung (DSGVO), insbesondere zum Schutz von Gesundheitsdaten nach Art. 9 DSGVO,
- ISO/IEC 27001:2022 als Grundlage des gemeinsamen ISMS,
- BSI-Anforderungskatalog Cloud Computing (C5) für die cloudbasierten SaaS-Produkte,
- branchenspezifische Anforderungen von KRITIS-Kunden (u. a. § 8a BSIG, § 391 SGB V, B3S Medizinische Versorgung) im Rahmen der Lieferantensteuerung,
- BSIG in der Fassung des NIS-2-Umsetzungsgesetzes, insbesondere §§ 30, 32 und 38 BSIG, für die medavis GmbH als wichtige Einrichtung,
- Cyber Resilience Act (CRA, Verordnung (EU) 2024/2847) für die Produkte der medavis GmbH.

Die konkrete Umsetzung dieser Anforderungen erfolgt in nachgelagerten Dokumenten (Sicherheitskonzepte, Richtlinien, Auftragsverarbeitungsverträge), die nicht Gegenstand dieser Leitlinie sind.

3. Sicherheitsziele

Die synava-Gruppe verarbeitet in nahezu allen Unternehmensbereichen schützenswerte Informationen, teilweise handelt es sich um Gesundheitsdaten. Der sichere Umgang mit diesen Informationen ist Grundlage für das Vertrauen von Kunden, Kostenträgern und Aufsichtsbehörden in die Produkte und Dienstleistungen der synava-Gruppe.

Da Ausfälle oder Manipulationen der bei medavis eingesetzten Systeme unmittelbar die radiologische und klinische Versorgung beeinträchtigen können, dient Informationssicherheit dort zugleich der Patientensicherheit. Die synava-Gruppe verfolgt daher folgende Sicherheitsziele:

Vertraulichkeit: Schützenswerte Informationen, insbesondere Gesundheitsdaten, werden wirksam vor unberechtigtem Zugriff und unbefugter Preisgabe geschützt.

Integrität: Die Vollständigkeit und Korrektheit von Informationen und die ordnungsgemäße Verarbeitung durch die eingesetzten IT-Systeme werden sichergestellt.

Verfügbarkeit: Die für die radiologische und klinische Versorgung erforderliche Verfügbarkeit von Systemen und Informationen wird gewährleistet, auch im Hinblick auf Notfall- und Wiederanlaufszszenarien bei Kunden mit KRITIS-Status.

Diese Ziele werden insbesondere erreicht durch die Verankerung der Informationssicherheit in der Unternehmensstrategie, sichere Entwicklungsprozesse für Eigenprodukte, ein systematisches Risiko- und Schwachstellenmanagement, Notfall- und Wiederanlaufplanung, die Steuerung von Subdienstleistern sowie regelmäßige Sensibilisierungs- und Schulungsmaßnahmen für alle Mitarbeitenden.

4. Sicherheitsorganisation

Informationssicherheit und Datenschutz sind bei der Verarbeitung von Gesundheitsdaten eng miteinander verzahnt. Die synava GmbH stellt daher für die gesamte Gruppe sicher, dass die folgenden Rollen mit klar abgegrenzten, aufeinander abgestimmten Verantwortlichkeiten besetzt sind. Die Gesamtverantwortung für die Informationssicherheit verbleibt bei der Geschäftsführung.

Chief Security & Compliance Officer (CSCO): steuert im Auftrag der Geschäftsführung Security & Compliance für beide Gesellschaften, stellt die Zusammenführung von Informationssicherheit und Datenschutz sicher und berichtet regelmäßig an die Geschäftsführung.

Informationssicherheitsbeauftragter (ISB): unterstützt den CSCO beim Betrieb des ISMS nach ISO/IEC 27001 und C5, insbesondere bei Dokumentation, Richtlinien, Auditplanung, Wirksamkeitsmessung und Risikobeurteilung. Der ISB berät Führungskräfte und Mitarbeitende und arbeitet eng mit der IT-Leitung zusammen.

Datenschutzbeauftragter (DSB): überwacht die Einhaltung der DSGVO bei der Verarbeitung personenbezogener Daten, berät Geschäftsführung und Fachbereiche in Datenschutzfragen und ist Ansprechpartner für Aufsichtsbehörden sowie betroffene Personen.

Bei Sicherheitsvorfällen mit Bezug zu personenbezogenen Daten stimmen sich CSCO, ISB und DSB unverzüglich ab, um die jeweiligen Melde- und Benachrichtigungspflichten (u. a. nach

Art. 33 und 34 DSGVO sowie ggf. branchenspezifische oder aufsichtsrechtliche Meldewege) koordiniert zu erfüllen. Der CSCO stellt die Zusammenarbeit der Rollen sicher, entscheidet über Meldungen an das BSI nach § 32 BSIg und eskaliert bei Bedarf an die Geschäftsführung.

5. Verbindlichkeit und Kommunikation

Diese Leitlinie sowie die daraus abgeleiteten Richtlinien, Konzepte und Verfahren sind von allen unter Ziffer 1.3 genannten Personen zu beachten und einzuhalten. Die Leitlinie wird allen Mitarbeitenden im Rahmen des Onboardings sowie über das Intranet zugänglich gemacht und regelmäßig im Rahmen von Awareness-Maßnahmen in Erinnerung gerufen. Verstöße gegen diese Leitlinie können arbeits-, vertrags- und im Einzelfall haftungsrechtliche Konsequenzen nach sich ziehen.

Ebenso wird die Leitlinie an Kunden und Lieferanten über die Webseite bekanntgegeben. Diese Leitlinie wurde von der Geschäftsführung der synava GmbH und der medavis GmbH herausgegeben und freigegeben.

Karlsruhe, 01.07.2026



Thomas Simon, CEO synava GmbH / CEO medavis GmbH