Datenschutz- und Datensicherheitskonzept
Prüfbericht 2024 / 2025

Diese Dokumentation dient als Nachweis für die Umsetzung die technischen und organisatorischen Maßnahmen der SEWOBE AG zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten. Damit erfüllt die SEWOBE AG die Anforderungen gemäß Artikel 32 Datenschutz-Grundverordnung (DSGVO) sowie die vertraglich vereinbarten Pflichten aus § 9 des Auftragsverarbeitungsvertrags.

Unternehmen / Auftragnehmer:	SEWOBE AG, Werner-Haas-Str. 8, 86153 Augsburg vertreten durch die Vorstände Eiko Trausch und Thomas Weishaupt (Verantwortliche i.S.d. Art. 4 DSGVO)
Prüfort:	Augsburg, Geschäftssitz: Werner-Haas-Str. 8, 86153 Augsburg
Prüfzeitraum:	1. Juni 2024 bis 31. Mai 2025
Prüfer / Koordination:	Datenschutz Serviceteam Augsburg, Dipl.-Ing. Heike Lenz, externe Datenschutzbeauftragte

INHALT

***Hinweis**: Im Prüfbericht findet das generische Maskulinum Anwendung, das alle weiteren Geschlechter miteinschließt.*

I. Gegenstand und Rechtsgrundlagen des Prüfberichts

Der vorliegende Prüfbericht dokumentiert für den Berichtszeitraum 2024/2025 die datenschutzrelevanten Maßnahmen, Prozesse und Entwicklungen innerhalb der SEWOBE AG im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen der Softwaredienstleistungen.

Gemäß dem zwischen der SEWOBE AG („Auftragnehmer“ oder auch „Auftragsverarbeiter“) und dem Kunden („Auftraggeber“ oder auch „Verantwortlicher“) geschlossenen Vertrag zur Auftragsverarbeitung (AV-Vertrag gemäß Art. 28 Abs. 3 DSGVO), verpflichtet sich die SEWOBE AG einmal jährlich einen Prüfbericht zu erstellen. Ziel dieses Berichts ist es, dem verantwortlichen Auftraggeber eine nachvollziehbare und belastbare Grundlage zur Erfüllung seiner gesetzlichen Kontroll- und Nachweispflichten zu bieten sowie die Umsetzung der technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DSGVO darzulegen.

Der AV-Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen zwischen dem Auftraggeber und dem Auftragnehmer und bezieht sich auf sämtliche Verarbeitungstätigkeiten, die im Zusammenhang mit der Nutzung der SEWOBE-Softwarelösungen stehen und bei denen Beschäftigte oder Beauftragte der SEWOBE AG Zugriff auf personenbezogene Daten des Kunden erhalten.

Der Prüfbericht ist in folgende Abschnitte unterteilt und wird den Kunden im Serviceportal zum Download bereitgestellt:

Kapitel II: Dokumentation individueller Maßnahmen zur Sicherstellung der datenschutzkonformen Verarbeitung und Gewährleistung der Sicherheit personenbezogener Daten.

Kapitel III: Darstellung der technisch-organisatorischen Maßnahmen der SEWOBE AG inklusive deren fortlaufender Evaluierung, Weiterentwicklung und Dokumentation im Datenschutzmanagementsystem (DSMS).

II. Individuelle Datenschutz- und Sicherheitsmaßnahmen

1. Datenschutz und IT-Sicherheit / Rolle der externen Datenschutzbeauftragten

Zur Sicherstellung eines durchgehend hohen Schutzniveaus hinsichtlich Datenschutzes und IT-Sicherheit setzt die SEWOBE AG auf ein umfassendes Maßnahmenkonzept. Ein zentraler Bestandteil dieses Konzepts ist die kontinuierliche Einbindung der externen Datenschutzbeauftragten in alle unternehmensrelevanten Prozesse.

Die Aufgaben der Datenschutzbeauftragten erstrecken sich über den gesamten administrativen Bereich – inklusive Personalprozesse – bis hin zu Softwareentwicklungen sowie der Auswahl und dem Einsatz von IT-Systemen und Infrastrukturkomponenten.

Ziel ist die konsequente Einhaltung der datenschutzrechtlichen Vorgaben in sämtlichen Verarbeitungsvorgängen personenbezogener Daten. Die Kontaktaufnahme mit der Datenschutzbeauftragten ist über datenschutz@sewobe.de möglich; die entsprechenden Kontaktdaten sind zudem öffentlich im Bereich „Datenschutzhinweise“ auf der Unternehmenswebsite einsehbar.

2. Einsatz von Künstlicher Intelligenz (KI)

Die SEWOBE AG nutzt Künstliche Intelligenz, um betriebliche Abläufe gezielt zu optimieren, fundierte datenbasierte Entscheidungen zu treffen und innovative Lösungsansätze für komplexe Herausforderungen zu realisieren.

Im Berichtszeitraum wurden zwei KI-gestützte Chatbots (sogenannte KI-Agents, z.B. Robbi) implementiert, die insbesondere dazu beitragen, die Informationsbereitstellung für Kunden zu verbessern und die Kommunikationsprozesse effizienter zu gestalten.

Bisher bezieht sich der Einsatz von KI auf reine Serviceanwendungen, dennoch werden Beschäftigte und Kunden angehalten, die Verwendung personenbezogener Daten bei Einsatz von KI zu unterlassen.

Transparenz und ein verantwortungsvoller Umgang mit KI-Technologien haben für die SEWOBE AG höchste Priorität. Entsprechend wird in den Datenschutzhinweisen umfassend über die Nutzung dieser Technologien und die damit verbundenen Maßnahmen informiert.

Für Juni 2025 ist die Weiterentwicklung der unternehmensinternen KI-Richtlinien vorgesehen. Diese erfolgt in enger Zusammenarbeit mit den Beschäftigten und unterliegt einer kontinuierlichen Überprüfung und Anpassung an techno-logische sowie regulatorische Entwicklungen.

3. Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO / Kontrollmechanismen

Zur systematischen Erfassung, Prüfung und Dokumentation aller relevanten Verarbeitungstätigkeiten personenbezogener Daten hat die SEWOBE AG detaillierte Verfahrensbeschreibungen sowie standardisierte Checklisten implementiert. Diese sind von den Beschäftigten verpflichtend zu bearbeiten und insbesondere vor Abschluss eines Projekts zur finalen Datenschutzprüfung vorzulegen.

Die vollständige und regelkonforme Dokumentation sämtlicher Verarbeitungstätigkeiten erfolgt im unternehmens-eigenen Datenschutzmanagementsystem (DSMS) und wird im Verzeichnis von Verarbeitungstätigkeiten (VVZ) gemäß Art. 30 DSGVO erfasst und regelmäßig aktualisiert.

Zur Fehlervermeidung, Prüfung und Aktualisierung wurden für alle wichtigen Verarbeitungstätigkeiten des Unternehmens personenbezogener Daten, Verfahrensbeschreibungen und Checklisten erstellt, die von allen Beschäftigten systematisch abzuarbeiten und u. a. vor Abschluss eines Projektes zur Prüfung vorzulegen sind, d. h., dass ein Vorgang erst nach Dokumentation aller hierfür notwendigen Vorgaben abgeschlossen werden darf. Alle erforderlichen Verarbeitungstätigkeiten werden im DSMS im Verfahrensverzeichnis (VVZ) hinterlegt.

4. Remote Work / Homeoffice: Regelungen, Schulungen und technische Absicherung

Zur Ermöglichung von Homeoffice-Arbeit unter Beibehaltung eines hohen Datenschutzniveaus gelten bei der SEWOBE AG strikte organisatorische und technische Vorgaben. Die Arbeit im Homeoffice ist gemäß Unternehmens-anweisung auf Tätigkeiten beschränkt, die keinen unmittelbaren Bezug zu personenbezogenen Daten aufweisen – etwa Softwareentwicklung oder interne technische Weiterentwicklungen. Kundenbezogene Projekte mit Personal-bezug, die der besonderen Datenkategorien angehören, sind vom Homeoffice aus nicht zulässig.
Ein Tätigwerden im Homeoffice ist für Beschäftigte und Werkstudenten grundsätzlich erst nach einer angemessenen Einarbeitungszeit zulässig, wenn die datenschutzkonforme Verarbeitung personen-bezogener Daten auch außerhalb der Unternehmensinfrastruktur sichergestellt ist. Auszubildenden ist das Arbeiten im Homeoffice bis zum Abschluss der Ausbildung grundsätzlich untersagt und nur in begründeten Einzelfällen möglich.

Alle Beschäftigten im Homeoffice haben Schulungen und Unterweisungen zu den erhöhten Gefahren im Homeoffice erhalten und wurden insbesondere zu regelmäßigen internen Sicherheitsprüfungen aller eingesetzten Betriebsmittel auf mögliche Bedrohungen informiert, die durch Schadsoftware und verstärkte Cyberangriffe erforderlich wurden. Sämtliche Betriebsmittel verfügen über sichere VPN-Verbindungen (virtuelles privates Netzwerk) und können per Fernwartung überprüft werden.

Um die zunehmende Bedrohung durch Cyberangriffe und die damit gestiegene reale Bedrohung für Remote- oder Homeoffice-Arbeitsplätze abzusichern, wurden während des Prüfungszeitraums die sicherheits-relevanten Vorgaben für die datenschutzkonforme Verarbeitung personenbezogener Daten im Homeoffice evaluiert und die damit verbundenen Unternehmensanweisungen, Verträge und Sicherheitsmechanismen der SEWOBE Beschäftigten angepasst.

Besondere Vorsicht gilt bei der Verarbeitung sensibler personenbezogener Daten im Sinne von Art. 9 DSGVO (z. B. Daten über politische Meinungen, Gewerkschaftszugehörigkeit oder Gesundheitsdaten). Projekte mit Bezug zu Organisationen aus diesen Bereichen (z. B. Parteien, Gewerkschaften, Religionsgemeinschaften, Gesundheitsinstitutionen) dürfen ausschließlich mit expliziter Genehmigung

der Geschäftsführung im Homeoffice durchgeführt werden – unter der Bedingung, dass ein unbefugter Zugriff durch Dritte technisch ausgeschlossen ist.

Homeoffice-Anträge müssen eine detaillierte Angabe der geplanten Projektinhalte enthalten und sind genehmigungspflichtig. Im Rahmen des dokumentierten Prüfungszeitraums wurden keine Verstöße festgestellt.

5. Datenschutzschulungen und -unterweisungen

Alle neuen Beschäftigten, einschließlich Werkstudenten und Praktikanten, erhalten am ersten Arbeitstag eine umfassende und dokumentierte Datenschutzschulung. Diese Schulung behandelt die wesentlichen Aspekte im Umgang mit personenbezogenen Daten. Ergänzend wird eine strukturierte „Welcome-Mappe“ ausgehändigt, die alle bislang implementierten Datenschutzmaßnahmen sowie Verhaltensregeln zur Zusammenarbeit im Unternehmen enthält.

Im Prüfzeitraum wurden sämtliche Beschäftigte mehrfach in sicherheitsrelevanten Themen unterwiesen, insbesondere in der korrekten Nutzung von Betriebsmitteln, der Notwendigkeit regelmäßiger Sicherheitsupdates (Firewall, Antivirenprogramme) sowie im sicheren Umgang mit Social Engineering-Risiken. Die Schulungen umfassten dabei unter anderem Bedrohungen durch Phishing-Mails, Schadsoftware wie Trojaner und Ransomware sowie die Risiken durch den Einsatz betriebsfremder USB-Sticks und anderen Speichermedien.

In internen Unternehmensrichtlinien ist verbindlich geregelt, dass der Download und die Nutzung nicht lizenzierter Software untersagt ist. Ebenso ist die regelmäßige Aktualisierung von Sicherheitsanwendungen sowie die Einhaltung technischer Schutzmaßnahmen verpflichtend. Das Onboarding- und Systemeinrichtungsteam ist für die stichprobenartige Überprüfung der Betriebsmittel sensibilisiert. Darüber hinaus ist die Installation von nicht datenschutzkonformen Hilfs- oder Drittanbieter-Apps untersagt.

Auszubildende werden im Rahmen der wöchentlichen, internen Schulungsveranstaltungen zusätzlich hinsichtlich Datenschutzes und Datensicherheit unterwiesen. Inhaltlich liegt der Fokus auf dem datenschutzkonformen Umgang mit Kunden- und Interessentendaten, insbesondere auf der korrekten Authentifizierung bei telefonischen Anfragen und Aufträgen. Die Schulungsinhalte werden praxisorientiert vermittelt, wobei gemeinsam mit den Auszubildenden geeignete Sicherheitsmaßnahmen erarbeitet und reflektiert werden.

6. Verpflichtung auf Vertraulichkeit / Geheimhaltungsvereinbarungen

Sämtliche Beschäftigte sowie externe Dienstleister der SEWOBE AG werden – je nach Art und Umfang ihrer Tätigkeit – vertraglich zur Wahrung der Vertraulichkeit, zur Einhaltung des Fernmeldegeheimnisses sowie zum Schutz von Geschäfts- und Betriebsgeheimnissen verpflichtet. Im Rahmen dieser Verpflichtung werden sie zudem über mögliche strafrechtliche Konsequenzen bei Verstößen gegen datenschutz- oder geheimnisschutzrechtliche Vorschriften belehrt. Die Vertraulichkeitsverpflichtung wirkt ausdrücklich auch über das Ende des Beschäftigungs- bzw. Dienstleistungsverhältnisses hinaus fort.

Für Sub- bzw. Unterauftragnehmer, die im Auftrag der SEWOBE AG personenbezogene Daten verarbeiten – etwa im Rahmen von Hosting-, Rechenzentrums- oder Cloud-Dienstleistungen –, werden Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO abgeschlossen. Diese Verträge stellen sicher, dass sämtliche Datenschutzvorgaben auch auf Ebene der beauftragten Dienstleister konsequent eingehalten werden. Eine Übersicht der aktuell eingesetzten Subunternehmer ist diesem Bericht im Anhang beigefügt und kann zusätzlich auf der Unternehmenswebsite unter dem Abschnitt „Datenschutz / Subunternehmer“ eingesehen werden.

7. Unternehmenskommunikation - Einsatz sicherer Softwareapplikationen und Medien

a. Unternehmensanweisungen

Die SEWOBE AG hat für alle Beschäftigten umfassende Unternehmensanweisungen etabliert, in denen verbindliche Regelungen zur Datensicherheit und zum Einsatz von IT-Systemen definiert sind. Im Prüfungszeitraum wurden diese Anweisungen aktualisiert, insbesondere im Hinblick auf die verpflichtende Nutzung ausschließlich lizenzierter Softwareprodukte, die regelmäßige Aktualisierung von Sicherheits-programmen sowie die Umsetzung technischer und organisatorischer Schutzmaßnahmen an den eingesetzten Betriebsmitteln. Die Einhaltung dieser Vorgaben wird durch stichprobenartige Kontrollen durch die IT-Abteilung in Zusammenarbeit mit der Datenschutzbeauftragten sichergestellt. Sämtliche Maßnahmen sind im Datenschutzmanagementsystem (DSMS) dokumentiert und den jeweiligen Verarbeitungstätigkeiten bzw. Verfahrensbeschreibungen zugeordnet.

b. Serviceportal vs. Kundenverkehr via E-Mail

Zur Reduzierung des Risikos von Schadsoftware-Angriffen wurde der direkte E-Mail-Kontakt mit Kunden weitgehend durch umfassenden Einsatz des SEWOBE Workflow-Ticketsystems im Serviceportal ersetzt. Diese Maßnahme ist inzwischen unternehmensweit etabliert. Eingehende externe E-Mails werden zudem automatisiert auf Schadsoftware geprüft; infizierte Anhänge werden systemseitig isoliert bzw. gelöscht, bevor sie verarbeitet oder angezeigt werden können.

c. Sichere Kommunikation

Für Kundenschulungen und digitale Meetings kommen ausschließlich sichere Kommunikationslösungen wie „TeamViewer“ oder „Microsoft Teams“ mit Serverstandorten in Deutschland oder der EU zum Einsatz. Dadurch wird sichergestellt, dass keine personenbezogenen Daten an Anbieter in Drittländern mit unzureichendem Datenschutzniveau übermittelt oder mitgeschnitten werden. Sollte ein Kunde explizit die Nutzung nicht-EU-konformer Kommunikationsplattformen (z. B. Zoom oder WebEx) wünschen, werden diese auf die datenschutzrechtlichen Risiken im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO hingewiesen. Trotz entsprechender Aufklärung bestehen einzelne Kunden weiterhin auf die Nutzung solcher Dienste; in diesen Fällen wird die Entscheidung dokumentiert und gesondert bewertet.

8. Evaluierung des Datenschutzmanagementsystem (DSMS) / Neu- und Weiterentwicklungen von Softwarefunktionen

Das digitale Datenschutzmanagementsystem (DSMS) der SEWOBE AG wird regelmäßig evaluiert, um gesetzlichen, technischen und organisatorischen Anforderungen kontinuierlich gerecht zu werden.
Während des Prüfungszeitraums wurde das Verzeichnis der Verarbeitungstätigkeiten (VVT) um neue Prozesse ergänzt und bestehende Einträge überarbeitet bzw. angepasst.

Insbesondere die Neu- und Weiterentwicklungen zentraler Softwarefunktionen und Zusatzmodule zur Optimierung der webbasierten Verwaltungsplattform wurden datenschutzseitig von der externen Datenschutzbeauftragten begleitet.
Bereits während der Entwicklungsphasen erfolgt eine datenschutzrechtliche Bewertung, um die Konformität mit der DSGVO sicherzustellen. In enger Zusammenarbeit mit dem Vorstand und der IT-Abteilung wird somit gewährleistet, dass der hohe Qualitäts- und Sicherheitsstandard der SEWOBE AG als Premiumanbieter digitaler Verwaltungssoftware auch in Zukunft eingehalten wird.

9. Notfallmanagement: Notfallplan / Notfallhandbuch

Aufgrund von längeren Stromausfällen in benachbarten EU-Staaten, aber auch in Augsburg im vergangenen Jahr, wurden die bestehenden Notfallsysteme gemeinsam mit dem internen Notfallteam erneut einer Prüfung unterzogen.
Der Notfallplan wurde aktualisiert und sowohl dem internen Notfallteam als auch sämtlichen Beschäftigten in verschiedenen Dateiformaten vorgehalten, um auch bei etwaigen Systemausausfall Zugriff auf alle erforderlich Kontaktdaten und Inhalte zu haben.in gedruckter Form sowie auf geeigneten Speichermedien zur Verfügung gestellt. Ziel ist es, im Ernstfall eine einheitliche Kommunikation sicherzustellen und einen strukturierten Wiederanlauf zu ermöglichen.

a. Notfallplan

Zentrales Ziel sämtlicher Maßnahmen des Notfallplans ist der Schutz personenbezogener Daten sowie die Minimierung von Ausfallzeiten und eine möglichst rasche Wiederaufnahme des Betriebs. Unterschiedliche Gefahrenlagen werden unter möglichst realen Bedingungen turnusmäßig simuliert und der Wieder-anlaufplan mit allen Beschäftigten abgestimmt. Dabei wird insbesondere der Wiederanlaufplan mit allen mit allen Beschäftigten aktualisiert, um im Ernstfall reibungslose Abläufe sicherzustellen.

Hierbei werden folgende verschiedene Krisenszenarien berücksichtigt:

- Cyberangriffe (Social Engineering)
- Einbruch / Diebstahl / Vandalismus
- Brand (Wasserschäden)
- Elementarschäden (Naturkatastrophen) / Überschwemmungen
- Ausfall von Führungspersonal – Vertretungsmanagement
- Akuter und längerer Stromausfall

Neben der Beschreibung potenzieller Gefahrenlagen enthält der Notfallplan eine strukturierte Dokumentation aller Unternehmensbereiche, inklusive zugeordneter Beschäftigter und Vertretungen. Durch regelmäßige Schulungen und Unterweisungen werden alle Beschäftigten befähigt, im Notfall regelkonform zu handeln.

Um auch bei technischen Störungen Zugriff auf alle relevanten Informationen zu gewährleisten, wird der Notfallplan in mehreren Dateiformaten (z. B. PDF, Office-Dokumente, Klartext-dateien) vorgehalten. Enthalten sind stets aktuelle Kontaktinformationen, verantwortliche Ansprechpartner sowie alternative Bürostandorte, um einen geordneten Geschäftsbetrieb zügig wiederherstellen zu können.

b. IT-Notfallhandbuch

Zur Sicherstellung eines strukturierten Systemwiederanlaufs – insbesondere nach schwerwiegenden Vorfällen wie Cyberangriffen – pflegt die SEWOBE AG ein IT-Notfallhandbuch. Dieses enthält detaillierte Anweisungen für das Vorgehen beim Wiederanlauf der IT-Infrastruktur und liegt sowohl in digitaler als auch in gedruckter Form vor. Die Pflege und Aktualisierung des Handbuchs erfolgten kontinuierlich unter Federführung der Vorstände.

c. Anpassung der baulichen Maßnahmen

Geplant sind zusätzliche bauliche Anpassungen, um mittels Photovoltaik-Anlage und Anschaffung eines entsprechend ausgelegtem Batteriespeicher möglichst lange autark weiterarbeiten bzw. den Stromausfall überbrücken zu können.

10. Allgemeine Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Datenschutz- und IT-Sicherheitsmaßnahmen (Art. 32 Abs. 1 lit. d DSGVO und Art. 25 Abs. 1 DSGVO)

Die SEWOBE AG hat – in Fortführung der Maßnahmen aus den Vorjahren – verschiedene etablierte Kontroll- und Evaluierungsverfahren implementiert, um die Datenschutzanforderungen und die Sicherheit der Verarbeitung im Rahmen der Technikgestaltung kontinuierlich zu gewährleisten und weiter zu entwickeln. Neben den in Ziffer 9 genannten Notfallkonzepten gibt es folgende weitere Verfahren:

a. Evaluierung der Datenschutz- und IT-Sicherheitskonzepte

Das unternehmensweite „Datenschutz- und IT-Sicherheitskonzept“ wird regelmäßig überprüft, aktualisiert und fortgeschrieben. Die Evaluierung erfolgt unter Einbeziehung der datenschutzrechtlich Verantwortlichen, der zuständigen Fachabteilungen sowie der bestellten Datenschutzbeauftragten. Ziel ist es, aktuelle Berichte über potenzielle Gefahren zu berücksichtigen und das Konzept zeitnah anzupassen.

b. System-Monitoring und technische Sicherheitsprüfungen

Zur laufenden Überwachung der Systemintegrität kommen sowohl eigenentwickelte Sicherheitsleistungen als auch das professionelle IT-Monitoring-System CheckMK zum Einsatz. Dieses ermöglicht eine umfassende Überwachung verschiedener Infrastrukturkomponenten, wie Server, Netzwerke, Anwendungen und Dienste. Die Überwachung erfolgt durchgängig (24/7) mittels automatisierter Monitoring-Systeme. Zusätzlich wird eine personelle Besetzung für die Systembeobachtung im Rahmen des Bereitschaftsdienstes sichergestellt – werktags von 7:00 bis 22:00 Uhr sowie an Wochenenden und Feiertagen von 10:00 bis 17:00 Uhr – um im Bedarfsfall unmittelbar intervenieren zu können.

c. Vertragsmanagement und rechtliche Evaluierung

In regelmäßigen Zyklen werden sämtliche Softwarelizenzverträge, Auftragsverarbeitungsverträge (AVV), unternehmensinterne Weisungen sowie begleitende Checklisten geprüft, aktualisiert und an geltende rechtliche sowie betriebliche Rahmenbedingungen angepasst. Dies umfasst sowohl datenschutzrechtliche als auch IT-sicherheits-relevante Vertragsbestandteile.

11. Zertifizierungen und Gütesiegel der SEWOBE Software Services (SoftwareMANAGER)

Die SEWOBE AG verfolgt konsequent einen qualitätsgesicherten Entwicklungsansatz und unterzieht ihre Software-lösungen regelmäßig unabhängigen Prüfverfahren und Zertifizierungen. Dies gewährleistet nicht nur die Einhaltung gesetzlicher und regulatorischer Vorgaben, sondern stärkt auch das Vertrauen von Kunden, Partnern und Aufsichts-behörden in die Leistungsfähigkeit und Sicherheit der eingesetzten Systeme.

a. IDW PS 880 Zertifizierung des Buchhaltungsmoduls

Die SEWOBE unterzieht sich seit März 2023 einem umfassenden Zertifizierungsverfahren gemäß IDW PS 880, basierend auf der spezifischen Richtlinie des Instituts der Wirtschafts-prüfer in Deutschland (IDW) mit dem Titel "Grundsätze ordnungsmäßiger Buchführung bei Einsatz von IT-Systemen (GoB IT)". Diese Richtlinie legt die Anforderungen fest, die ein Buchführungssystem erfüllen muss, um den Grundsätzen ordnungsmäßiger Buchführung (GoB) zu entsprechen.
Die Vorteile des anerkannten Verfahrens sind vielfältig, u.a.:

- Die IDW PS 880-Zertifizierung ist ein anerkannter Standard in der Buchhaltungsbranche
- Rechtssicherheit: Eine zertifizierte Software überprüft die gesetzlichen Anforderungen und Vorschriften für die Buchführung
- Die Richtlinie legt auch Anforderungen an die Funktionalität und Sicherheit des Buchhaltungs-systems fest und sorgt für nachhaltige und effiziente Prozesse in der Buchhaltung.
- Kontinuierliche Verbesserung der Buchhaltung durch regelmäßigen Audit

Seit der letzten Zertifizierung wurden die geprüften Bereiche der Buchhaltung optimiert und erweitert, z.B. um die E-Rechnung angepasst. Eine Überprüfung der Zertifizierung ist geplant, sobald umfangreichere Optimierungen des Buchhaltungsmoduls umgesetzt werden (z. B. DATEV-Schnittstellen, SKR 42).

b. „Trusted Cloud e. V."

Die SEWOBE AG hat Ihre SoftwareMANAGER bzw. Services (SoftwareMANAGER) wiederholt erfolgreich überprüfen lassen. Hierbei handelt es um einen zertifizierten Service des Kompetenznetzwerk Trusted Cloud e. V. Dieses Label wurde auf Initiative des Bundesministeriums für Wirtschaft und Energie auf Wunsch der Mittelständischen Wirtschaft entwickelt, um einen abgesicherten und qualifizierten Industriestandard zu schaffen. Im Vordergrund des Trusted Cloud Labels steht die Schaffung von Transparenz bzw. die Förderung des Vertrauens in Cloud-Technologien. Geprüft wird der
Transfer von anwenderorientiert aufgebautem Wissen rund um das Cloud Computing und die Listung von geprüften Cloud-Anwendungen. Das Kompetenznetzwerk Trusted Cloud e.V. fördert somit den effizienten, sicheren und rechts-konformen Einsatz von Cloud-Technologien: https://www.trusted-cloud.de/.

Weitere Detail-Informationen zur MANAGER Zertifizierung finden Sie hierzu auf der Website: https://www.trusted-cloud.de/cloudservices/2159/

c. SOFTWARE MADE IN GERMANY“ und „SOFTWARE HOSTED IN GERMANY

Die SEWOBE AG ist geprüfte Inhaberin der Gütesiegel „SOFTWARE MADE IN GERMANY“ und „SOFTWARE HOSTED IN GERMANY“, eine Initiative des Bundesverbands IT-Mittelstand (BITMi e.V.). Folgende Kriterien sind zu erfüllen: In Deutschland programmierte und designte Software, deutsch- sprachige Hotline und Schulungen / Sicherstellung der Kompatibilität der Programme und Daten / Updates werden vertraglich zugesichert u.v.m. Weitere Detail-Informationen zur MANAGER Zertifizierung finden Sie hierzu auf der Website: https://www.software-made-in-germany.org

d. DATEV Schnittstelle

Pünktlich zum Jahreswechsel 24/25 wurde die Online-DATEV-Schnittstelle von DATEV-zertifiziert. Die erfolgreiche Integration des DATEV Buchungsdatenservices in die SEWOBE MANAGER-Softwarelösungen ermöglicht es den Kunden, eine nahtlose und effiziente Zusammenarbeit mit DATEV.

12. Änderungen von Zugriffsberechtigungen innerhalb einer Organisation des Auftraggebers - Erteilung oder Entzug von Zugriffsberechtigungen (z.B. Vorstandswechsel)

Im Prüfzeitraum gingen erneut bei der SEWOBE AG wiederholt Mitteilungen von Organisationen (im Rahmen des Vertragsverhältnisses auch als Kunden oder Auftraggeber bezeichnet) per E-Mail oder Brief ein, mit der Aufforderung, Zugriffsrechte für bisher berechtigte Personen zu entziehen.

Um Rechtssicherheit zu schaffen, wurde im Softwaremietvertrag ein Zusatz aufgenommen, der Organisationen ausdrücklich verpflichtet, Veränderungen von Zugriffsberechtigungen eigenständig über die Verwaltungsoberfläche der Software zu dokumentieren und zu verwalten. Eine Kommunikation über nicht vertraglich vereinbarte Kanäle (z. B. formloser E-Mail-Verkehr) ist ausgeschlossen und wird aus Gründen der Datensicherheit und Nachvollziehbarkeit nicht akzeptiert.

Die SEWOBE AG handelt im Rahmen der Auftragsverarbeitung (Art. 28 DSGVO) ausschließlich weisungsgebunden und ist vertraglich verpflichtet, Berechtigungen ausschließlich auf Grundlage autorisierter, eindeutig nachvollziehbarer Anweisungen zu ändern. Änderungen von Benutzer- und Zugriffsrechten, die nicht über das integrierte Berechtigungsmanagement innerhalb der SEWOBE-Software oder über das offizielle Serviceportal eingetragen und übermittelt wurden, können daher nicht umgesetzt werden, solange keine hinreichende Legitimation vorliegt.

Voraussetzung für die Bearbeitung von Berechtigungsänderungen:
- Schriftlicher Antrag mit nachvollziehbarem Nachweis der Berechtigung (z. B. beglaubigter Vorstandsbeschluss oder Handels-/Vereinsregisterauszug)
- Vorlage eines gültigen Identitätsnachweises des Antragsstellers
- Eindeutige Bestätigung, dass der Antragsteller bevollmächtigt ist, Zugriffsbefugnisse zu erteilen, zu ändern oder zu entziehen

Die SEWOBE AG behält sich im Zweifelsfall das Recht vor, Anträge bis zur vollständigen Klärung und Vorlage aller erforderlichen Nachweise zurückzustellen, da eine eigenständige Bewertung von Berechtigungskonstellationen nicht Bestandteil des Auftragsverhältnisses ist.

Anlage

Kapitel III. Technische und organisatorische Maßnahmen

III. Technische und organisatorische Maßnahmen

gemäß Art. 32 DSGVO i. V. m. Erwägungsgrund 78

Stand 06.2025

Die jeweils aktuelle Version der Technischen und Organisatorischen Maßnahmen (TOM) der SEWOBE AG ist Bestandteil des Auftragsverarbeitungsvertrags und wird Neukunden gemeinsam mit dem Softwaremietvertrag zur Verfügung gestellt. Aus Gründen der Datensicherheit gilt für Bestandskunden stets die zum jeweiligen Zeitpunkt aktuelle Fassung der TOM.

1. Sicherheitsmaßnahmen der SEWOBE AG / SoftwareMANAGER-Lösungen

Zum Schutz sensibler Informationen und zur Sicherstellung einer rechtskonformen und zuverlässigen Kommunikation hat die SEWOBE AG umfassende organisatorische und technische Sicherheitsmaßnahmen implementiert. Diese Maßnahmen gelten sowohl unternehmensintern als auch innerhalb der Softwarelösungen für Kunden und Partner.

1.1. Zugriffsregularien bei Systemzugang / Mehrfaktor-Authentifizierung (MFA) / Newsletter-Versand

Zur Absicherung aller Zugänge zu den SoftwareMANAGER-Anwendungen wird eine mehrstufige Authentifizierung eingesetzt. Die Kombination aus Passwort und einem zweiten Authentifizierungsfaktor (z. B. per Authenticator-App oder SMS) schützt den Zugriff auf sensible Daten wirksam vor unautorisierten Zugriffen.

Für den Zugang zur Verwaltungssoftware sowie für Funktionen wie den Versand von Newslettern sind somit folgende Sicherheitsmaßnahmen empfohlen:

- das Double-Opt-in-Verfahren bei E-Mail-Adressen,
- die Prüfung der Adressinhaberschaft,
- sowie die Zwei-Faktor-Authentifizierung

Diese Maßnahmen werden im Rahmen von Anwenderschulungen aktiv vermittelt. Ziel ist es, die Integrität der Kommunikationskanäle sowie die Echtheit der verwendeten E-Mail-Adressen sicherzustellen.

1.2. Gesicherte Kommunikation über das Serviceportal

Die SEWOBE AG hat aus sicherheits- und datenschutzrechtlichen Gründen die klassische E-Mail Kommunikation mit Kunden weitgehend eingestellt. Sämtliche Support- und Kommunikationsprozesse werden über das SEWOBE-Serviceportal abgewickelt, dessen Nutzung vertraglich verpflichtend im Softwarenutzungsvertrag geregelt ist.

Das SEWOBE-Serviceportal bietet einen passwortgeschützten, verschlüsselten Zugang für Kunden und deren autorisierte Vertreter. Darüber können sicherheitskritische Vorgänge wie:

- Support-Anfragen,
- Austausch sensibler Daten sowie
- Nutzung eines geschützten Dokumentenarchivs

abgewickelt werden. Kunden sind ausdrücklich angewiesen, keine sensiblen Informationen per E-Mail zu übermitteln. Trotz dieser vertraglichen Vorgabe kam es im Prüfungszeitraum wiederholt zu Verstößen durch einzelne Kunden. In diesen Fällen erfolgt eine dokumentierte Ansprache der zuständigen Ansprechpartner bzw. Datenschutzbeauftragten. Diese Praxis wird konsequent

fortgesetzt. Neukunden werden im Onboarding explizit über die Risiken der E-Mail-Kommunikation informiert und auf die verpflichtende Nutzung des Portals hingewiesen.

Neukunden werden in Kundengesprächen verstärkt für ggf. resultierende Gefahren aus der E-Mail-Kommunikation sensibilisiert und auf die Nutzungsvereinbarungen hingewiesen.

1.3. Systemzugang SoftwareMANAGER, Newsletter-Versand bzw. E-Mail-Kommunikation

Nach wiederholten Hinweisen haben sich zwischenzeitlich das Double-Opt-in Verfahren und die 2-Faktor-Autentifizierung etabliert, jedoch nicht bei allen Auftraggebern. In Schulungen weisen die Beschäftigten der SEWOBE die Anwender des Auftraggebers auf diese erforderlichen Sicherheitsmaßnahmen hin. Auf diese Weise kann überprüft werden, dass die angegebenen E-Mail-Adressen in den Newsletter-Anträgen auch identisch mit den tatsächlichen Inhabern der E-Mail-Adressen sind. Auch der Systemzugang zur Verwaltungssoftware ist Mehrfaktorauthentifizierung und Passwort gesichert.

1.4. Sicherheitsaspekte im Mitglieder- bzw. Kundenportal

Das optionale Mitglieder- bzw. Kundenportal (verfügbar in den Versionen „Pro“ und „Pro Plus“) ermöglicht die sichere Bereitstellung personenbezogener Informationen innerhalb der Kundenorganisation. Dokumente mit potenziell sensiblen Inhalten können hier zentral, zugriffsgeschützt und datenschutzkonform bereitgestellt werden – ohne Versand über unsichere Kommunikationswege wie E-Mail. Dies erhöht die Datensicherheit erheblich und unterstützt eine DSGVO-konforme Datenverarbeitung.

2. Vertraulichkeit

Zur Wahrung der Vertraulichkeit personenbezogener Daten setzt die SEWOBE AG umfassende technische und organisatorische Maßnahmen ein, um unbefugte Zugriffe auf gespeicherte oder übermittelte Daten zu verhindern. Ziel ist es, eine unrechtmäßige Informationsgewinnung durch Dritte konsequent auszuschließen und die Integrität der Datenverarbeitung zu gewährleisten.
Diese Maßnahmen gewährleisten ein hohes Maß an Zugriffsschutz und tragen wesentlich zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit verarbeiteter personenbezogener Daten sowie unternehmensrelevanter Informationen bei.

2.1. Zutrittskontrolle

Zur Verhinderung des unbefugten physischen Zutritts zu Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet oder gespeichert werden, setzt die SEWOBE AG an ihrem Geschäftssitz folgende Sicherheitsmaßnahmen um:

- Elektronisches Zutrittskontrollsystem mit Videoüberwachung:
  Der Zugang zu den Geschäftsräumen erfolgt ausschließlich über ein elektronisches Schließsystem mit individueller Zutrittsberechtigung für autorisierte Beschäftigte. Der Zutritt wird protokolliert; die gespeicherten Daten werden in regelmäßigen Intervallen datenschutzkonform gelöscht. Zusätzlich ist der Eingangsbereich kameraüberwacht. Mit dem Anbieter der Zutrittslösung besteht ein Vertrag zur Auftragsverarbeitung (AVV) gemäß Art. 28 DSGVO.
- Zugangsbeschränkungen:
  Externe Besucher erhalten nur nach vorheriger Anmeldung Zutritt zu den Geschäftsräu-

men. Sie werden am Empfang (Frontoffice) persönlich in Empfang genommen und überprüft. Eine freie Bewegung innerhalb der Räumlichkeiten ist nicht möglich. Der Aufenthalt erfolgt ausschließlich in Begleitung autorisierter Beschäftigter.

- Absicherung sensibler Bereiche:
  Räume mit besonders schützenswerter Infrastruktur, wie z. B. der Serverraum, sind zusätzlich durch elektronische Hochsicherheitsschlösser geschützt. Der Zugang ist auf einen eng definierten Personenkreis beschränkt und wird ebenfalls protokolliert.
- Verbindliche Regelungen zur Raumnutzung:
  Für Beschäftigte, autorisierte Dritte sowie Dienstleister und Gäste / Besucher bestehen verbindliche schriftliche Vorgaben zur Nutzung und zum Verhalten in den Geschäftsräumen.
- Kameraüberwachung sicherheitskritischer Bereiche:
  Die Videoüberwachung erstreckt sich auf den Eingangsbereich, Flure, Büroabschlusstüren sowie auf alle Räume mit sicherheitsrelevanter Infrastruktur. Die Aufzeichnung erfolgt im Einklang mit den datenschutzrechtlichen Vorgaben.

2.2. Zugangskontrolle

Der physische Zugang zu IT-Systemen und Datenverarbeitungseinrichtungen (z. B. Server, Workstations, Netzwerkkomponenten) ist durch ein mehrstufiges Zugriffsmanagement geregelt, das den unautorisierten Zugriff systematisch verhindert. Die Implementierung erfolgt unter Einhaltung datenschutzrechtlicher und informationssicherheitsrelevanter Anforderungen, insbesondere gem. Art. 32 DSGVO sowie auf Basis anerkannter Standards. Folgende technische und organisatorische Maßnahmen (TOM) zur Zugangskontrolle werden verbindlich angewendet:

- Benutzerauthentifizierung mittels individueller Zugangsdaten (Benutzername und Passwort)
- Obligatorische Zwei-Faktor-Authentifizierung (2FA**)** für privilegierte Zugänge und externe Verbindungen
- Richtlinien zur Passwortkomplexität**:** Verwendung von Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern mit einer Mindestlänge von acht Zeichen
- Regelmäßige Passwortwechsel gemäß definiertem Fristen sowie Sperrung historischer Passwörter
- Begrenzung der Anzahl zulässiger Fehlversuche, um Brute-Force-Angriffe zu verhindern
- Definierte Wechselfristen, Passworthistorie
- Automatische Bildschirmsperrung bei Inaktivität**,** reaktivierbar nur durch erneute Authentifizierung
- Etablierung von Kontroll-, Prüf- und Abstimmmechanismen, insbesondere durch Login, Monitoring und regelmäßige Re-Zertifizierung von Benutzerrechten

2.3 Zugriffskontrolle

Die Zugriffskontrolle stellt sicher, dass ausschließlich berechtigte Personen auf Datenverarbeitungssysteme und darin verarbeitete personenbezogene sowie vertrauliche Informationen zugreifen können. Ziel ist die wirksame Verhinderung unzulässiger Verarbeitungstätigkeiten wie unbefugtes Lesen, Kopieren, Verändern oder Löschen von Daten außerhalb der jeweils zugewiesenen Berechtigungen. Diese Maßnahmen gewährleisten ein wirksames Zugriffsschutzniveau und tragen zur Einhaltung der datenschutzrechtlichen Vorgaben gemäß Art. 5 Abs. 1 lit. f sowie Art. 32 DSGVO bei. Die SEWOBE AG setzt hierzu folgende technische und organisatorische Maßnahmen (TOM) ein:

- Physische Sicherheit von Datenträgern: Aufbewahrung von Datenträgern erfolgt gesichert in abschließbaren Aufbewahrungseinheiten bzw. Serverräumen.
- Berechtigungs- und Rollenkonzept in der SoftwareMANAGER-Suite: Die Anwendungen der

SEWOBE AG verfügen über ein differenziertes Berechtigungsmanagement mit der Möglichkeit zur Erstellung und Verwaltung von Benutzerprofilen. Zugriffsrechte sind rollenbasiert zuweisbar und über eine Rechtehistorie revisionssicher nachvollziehbar.

- Netzwerksicherheit durch technische Schutzmaßnahmen: Einsatz von professionellen Firewall-Systemen und Antivirenlösungen mit automatisierten Sicherheitsupdates und Patching zur Absicherung gegen externe Angriffe und Schadsoftware.
- Restriktive Administratorrechtevergabe: Administrationsrechte werden nach dem Minimalprinzip vergeben („Least Privilege“). Die Vergabe wird protokolliert und unterliegt der Kontrolle durch den technischen Vorstand.
- Sicherer Fernzugriff mittels VPN-Technologie: Mobile Endgeräte sind ausschließlich über verschlüsselte VPN-Verbindungen an das interne Netz angebunden, um eine gesicherte Kommunikation zu gewährleisten.
- Gerätesicherheit durch Festplattenverschlüsselung: Alle mobilen Endgeräte sind durch moderne Festplattenverschlüsselungstechnologien gegen unbefugten Datenzugriff bei Verlust oder Dieb-stahl geschützt.
- Organisatorische Richtlinien: Etablierte Arbeitsanweisungen und definierte Bearbeitungsprozesse für den Umgang mit Datenverarbeitungsvorgängen sichern die einheitliche und regelkonforme Datenverarbeitung.
- Absicherung von Schnittstellen: USB-Schnittstellen sind systemseitig kontrolliert bzw. eingeschränkt nutzbar. Datenübertragungen erfolgen ausschließlich verschlüsselt.
- Verschlüsselung mobiler Datenträger: Externe Datenträger (z. B. USB-Sticks, externe SSDs) unterliegen einer verpflichtenden Verschlüsselung.
- Sicherheitsmechanismus der Softwareanwendung: Die „Historie“ protokolliert alle Zugriffe auf Anwendungen.
- Kontrollierte physische Vernichtung von Datenträgern durch zertifizierte Unternehmen (Zertifikate z.B. von Documentus Bayern / Reisswolf)
- Clear-Desk-Policy: Die Einhaltung der Clear-Desk-Policy wird regelmäßig kontrolliert, um eine unbeabsichtigte Offenlegung sensibler Informationen im Arbeitsumfeld zu vermeiden.

2.4 Trennungskontrolle

Technische und organisatorische Maßnahmen zur Gewährleistung der Vertraulichkeit von personenbezogenen Daten während der Übertragung und zur Vermeidung unbefugter Zugriffe durch Dritte:

- Einsatz separater Serverinstanzen zur Mandantentrennung, physikalisch getrennte Infrastrukturen für unterschiedliche Verarbeitungszwecke sowie geografisch verteilte Backup-Standorte zur Minimierung von Zugriffskonflikten.
- Mandantenspezifische Datenhaltung: Implementierung einer strikt mandantenbasierten Datenmodellierung in der Applikations- und Datenbankarchitektur, inklusive eindeutiger Mandantenzuweisung auf Tabellen- und Schemaebene.
- Differenzierte Datenbank- und Systemberechtigungen: Rollenspezifische Vergabe von Zugriffsrechten durch autorisierte Stellen (z. B. CIO), um eine klare organisatorische und technische Trennung der Verantwortlichkeiten zu gewährleisten.
- Umgebungstrennung für Entwicklungs-, Test- und Produktivsysteme: Strikte Isolation von Test- und Produktionsumgebungen zur Vermeidung von Datenvermischung und zur Einhaltung von Compliance-Vorgaben.

2.5 Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO; Art. 25 Abs. 1 DSGVO)

Maßnahmen, die sicherstellen, dass während der Übertragung ein Auslesen durch unbefugte Dritte nicht möglich ist:

- Transportverschlüsselung durch SSL/TLS-Zertifikate: Einsatz aktueller kryptografischer Protokolle zur Absicherung sämtlicher Netzwerkkommunikation, insbesondere bei Webportalen, APIs und servergestützten Anwendungen.
- Nutzung sicherer Kommunikationskanäle: Sensible Datenübermittlungen erfolgen ausschließlich über das geschützte SEWOBE Serviceportal oder ein zertifiziertes Ticketsystem. Die Übertragung über unsichere Medien wie E-Mail, USB-Sticks oder andere portable Datenträger ist unterbunden bzw. organisatorisch ausgeschlossen.
- Implementierung eines Bewerberportals zur sicheren Übermittlung von sensiblen Beschäftigtendaten.
- Einsatz eines datenschutzkonformen Bewerberportals: Zur sicheren und verschlüsselten Übermittlung personenbezogener Bewerbungsunterlagen kommt ein speziell entwickeltes Online-Portal zum Einsatz, das den Schutz sensibler Beschäftigtendaten gemäß DSGVO sicherstellt.

3. Integrität / Authentizität

Technische und organisatorische Maßnahmen zur Sicherstellung der Korrektheit, Nachvollziehbarkeit, Unveränderbarkeit und Verlässlichkeit von Informationen, Systemen und Verarbeitungsergebnissen. Ziel ist es, Datenverfälschung, Systemmanipulationen und fehlerhafte Resultate aufgrund von Hard- oder Softwarefehlern zu verhindern.

3.1. Weitergabekontrolle

Technische und organisatorische Maßnahmen zur Verhinderung unbefugter Einsichtnahme, Manipulation, Vervielfältigung oder des Verlusts von Daten bei Übertragung und Speicherung sowie zur Nachvollziehbarkeit der Datenweitergabe:

- Bevorzugte Übertragung über sichere Kanäle: Versand personenbezogener Dokumente (z. B. Verträge) bevorzugt über das SEWOBE Serviceportal oder auf dem Postweg; Absicherung durch dedizierte Standleitungen bzw. verschlüsselte VPN-Verbindungen bei elektronischer Kommunikation.
- Technische Schutzmechanismen: Einsatz aktueller Firewall-Technologien, regelmäßig aktualisierter Antiviren- und Endpoint-Protection-Lösungen zur Absicherung der IT-Infrastruktur gegen Schadsoftware und unbefugten Zugriff.
- Empfängerdokumentation: Vollständige Protokollierung und Dokumentation von Datenweitergaben inkl. Zweckbindung, Löschfristen und Datenarten – z. B. im Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO.
- Nachweisbare Identitätsprüfung: Protokollierte Authentifizierung und Autorisierung der empfangenden Stellen; optional mit Zwei-Faktor-Authentisierung und/oder qualifizierter elektronischer Signatur.
- Asset-Management und IT-Inventarisierung: Zentrale Erfassung und fortlaufende Pflege von eingesetzten Hard- und Softwarekomponenten im Inventarverwaltungssystem zur Nachverfolgbarkeit und Compliance-Sicherung.
- Ausnahmeregelung bei E-Mail-Kommunikation: Falls technisch oder organisatorisch notwendig, erfolgt die verschlüsselte Übermittlung von Daten per E-Mail ausschließlich in verschlüsselten ZIP-Containern und nur nach ausdrücklicher Zustimmung der betroffenen Partei – standardmäßig wird das SEWOBE Serviceportal verwendet.
- Entsorgung von Festplatten, Disketten und Akten durch zertifizierte Unternehmen und entsprechende Nachweise
- Sensibilisierung und Schulung: Regelmäßige Unterweisungen der Beschäftigten zur Einhaltung der Zweckbindung und zur Vermeidung unbeabsichtigter Datenweitergaben im Rahmen der datenschutzrechtlichen Verantwortlichkeiten.

- Verzicht auf mobile Speichermedien: Unternehmensweite Policy zum Ausschluss des Einsatzes mobiler Datenträger wie USB-Sticks, externen Festplatten oder unverschlüsselten Wechselmedien zur Minimierung des Risikos von Datenverlust oder Datendiebstahl.

3.2. Eingabekontrolle / Verarbeitungskontrolle

Technische und organisatorische Maßnahmen zur Sicherstellung der Nachvollziehbarkeit, wer zu welchem Zeitpunkt personenbezogene Daten erfasst, verändert oder gelöscht hat. Ziel ist es, Manipulationen zu verhindern sowie eine revisionssichere Protokollierung zu gewährleisten:

- Zugriffs- und Berechtigungsmanagement: Einsatz standardisierter Checklisten zur strukturierten Vergabe, Änderung und Entziehung von Zugangsrechten und Benutzerberechtigungen für den SEWOBE SoftwareMANAGER. Die Rechtevergabe erfolgt rollenbasiert nach dem Prinzip der minimalen Rechtevergabe („Need-to-know“).
- Automatisierte Protokollierung aller Verarbeitungsschritte: Lückenlose Aufzeichnung sämtlicher Eingabe-, Änderungs- und Löschvorgänge durch die integrierte Historienfunktion der SEWOBE Software. Die Protokolle enthalten u. a. Benutzerkennung, Zeitstempel, betroffene Datensätze sowie Art und Umfang der vorgenommenen Änderung.
- Revisionssichere Verarbeitungshistorie: Die Verarbeitungshistorie erlaubt die eindeutige Identifikation des jeweils verantwortlichen Nutzers sowie die zeitliche Einordnung einzelner Vorgänge – inkl. Dauer, Bearbeitungszeitpunkt und Nutzeraktion.
- Erweiterte Auswertungs- und Reporting-Funktionalitäten: Möglichkeit zur Erstellung individueller Protokolle und Auswertungen über sämtliche verarbeitete Daten und Aktivitäten innerhalb der Anwendung, zur Unterstützung interner Kontrollmechanismen sowie externer Datenschutzprüfungen.
- Integrierte Scan- und Upload-Funktionalitäten: Einsatz von validierten Schnittstellen zur digitalen Erfassung von Dokumenten über integrierte Scanner- oder Upload-Module. Dies reduziert Medienbrüche, minimiert manuelle Eingabefehler und erhöht den Schutz vor unautorisierten Datenmanipulationen.

3.3. Dokumentationskontrolle

Organisatorische Maßnahmen zur Sicherstellung der Transparenz, Nachvollziehbarkeit und Revisionssicherheit bei der Verarbeitung personenbezogener Daten:

- Organisatorische Maßnahmen zur Sicherstellung der Transparenz, Nachvollziehbarkeit und Revisionssicherheit bei der Verarbeitung personenbezogener Daten:
- Erfassung eingesetzter IT-Systeme und Systemkonfigurationen: Vollständige Dokumentation der im Verarbeitungsprozess eingesetzten Hard- und Softwaresysteme inklusive Versionsstände, technischer Konfigurationsparameter und personengebundener Systemzuweisungen (z. B. Administratoren, Systemverantwortliche) zur Sicherstellung der technischen Nachvollziehbarkeit und Verantwortlichkeitszuordnung.

3.4. Auftragskontrolle

Sicherstellung der datenschutzkonformen Verarbeitung personenbezogener Daten durch den Auftragnehmer:

- Sämtliche Tätigkeiten des Auftragnehmers erfolgen ausschließlich auf Grundlage eines gültigen Vertrags zur Auftragsverarbeitung gemäß Art. 28 DSGVO oder auf explizite Weisung des Auftraggebers im Rahmen eines erteilten Einzelauftrags.
- Die formale Erteilung von Aufträgen erfolgt ausschließlich über das SEWOBE-Ticketsystem. Eine Bearbeitung beginnt erst nach ausdrücklicher Freigabe durch eine berechtigte Person.
- Mündlich erteilte Aufträge sind vom Auftraggeber unverzüglich schriftlich zu bestätigen.

- Vor Annahme eines Auftrags prüft der Auftragnehmer die Berechtigung des Auftraggebers. Berechtigte Personen sind sowohl im zugrundeliegenden Vertrag als auch in der SEWOBE-Softwarelösung hinterlegt.
- Die formale Erteilung von Aufträgen erfolgt ausschließlich über das SEWOBE-Ticketsystem. Eine Bearbeitung beginnt erst nach ausdrücklicher Bestätigung.
- Für Fernwartungszwecke kommen ausschließlich Lösungen wie TeamViewer oder Microsoft Teams zum Einsatz, wobei sich die verwendeten Serverstandorte innerhalb Deutschlands bzw. der Europäischen Union befinden müssen.
- Die zulässigen Kommunikationskanäle werden in Abhängigkeit von den jeweiligen Serverstandorten innerhalb der EU definiert und dokumentiert.
- Beide Vertragsparteien verpflichten sich zur Einhaltung angemessener technischer und organisatorischer Datenschutzmaßnahmen, mindestens in gleichwertigem Umfang gemäß den Anforderungen der DSGVO.

4. Verfügbarkeit und Belastbarkeit

Zur Gewährleistung eines durchgängig hohen Schutz- und Verfügbarkeitsniveaus der verarbeiteten personenbezogenen Daten sowie der eingesetzten IT-Infrastruktur setzt die SEWOBE AG folgende technische und organisatorische Maßnahmen um.

4.1. Verfügbarkeitskontrolle

- Einsatz unterbrechungsfreier Stromversorgungen (USV-Anlagen) sowie von Überspannungsschutzsystemen; Überprüfung und Optimierung der Infrastruktur infolge des Stromausfalls Ende Mai 2025 nach Austausch im Jahr 2024.
- Betrieb einer klimatisierten Serverumgebung mit permanenter Online-Überwachung von Temperatur und Luftfeuchtigkeit.
- Verwendung spezieller Schutzsteckdosen im Serverraum zur zusätzlichen Absicherung der Hardwarekomponenten.
- Bereitstellung von Feuerlöschgeräten an strategisch relevanten Punkten in den Räumlichkeiten der SEWOBE AG.
- Installation von Rauch- und Brandmeldern zur frühzeitigen Detektion potenzieller Gefahrenquellen.
- Implementierung regelmäßiger, standortübergreifender Backup-Strategien zur Sicherstellung der Datenverfügbarkeit auch im Katastrophenfall.
- Kameraüberwachung sicherheitsrelevanter Infrastrukturbereiche zur Prävention unbefugter Zugriffe.
- Einsatz professioneller Firewall-Lösungen sowie kontinuierlich aktualisierter Virenschutzsysteme zum Schutz vor Cyberbedrohungen.
- Regelmäßige Überprüfung, Evaluierung und Weiterentwicklung des unternehmensweiten Notfallmanagements, einschließlich eines dokumentierten Wiederanlaufplans (Disaster Recovery Plan).
- Abschluss von Verträgen zur Auftragsverarbeitung gemäß Art. 28 DSGVO mit allen beteiligten Rechenzentrumsdienstleistern zur Sicherstellung eines angemessenen Datenschutzniveaus.

4.2. Belastbarkeit (Widerstandsfähigkeit von Systemen und Dienstleistungen)

Widerstandsfähigkeit technischer Systeme und Dienstleistungen gegenüber Störungen und Teilausfällen

Zur Sicherstellung der kontinuierlichen Verfügbarkeit sowie zur Aufrechterhaltung der

Funktionsfähigkeit kritischer Systeme und Prozesse auch im Falle von Betriebsstörungen oder Teilausfällen setzt die SEWOBE AG folgende Maßnahmen um:

- Implementierung von Schutzmechanismen zur Vermeidung von Systemüberlastungen sowie regelmäßige Durchführung von Penetrationstests zur Identifikation potenzieller Schwachstellen und zur Prüfung der System-Resilienz.
- Einsatz redundanter Systemarchitekturen zur Minimierung von Ausfallrisiken und zur Gewährleistung eines unterbrechungsfreien Betriebs.
- Entwicklung und Pflege eines umfassenden Ausfallsicherheits- bzw. Hochverfügbarkeitskonzepts zur strukturierten Reaktion auf Störungen und zur raschen Wiederherstellung der Systemverfügbarkeit.

- Verwendung fehlertoleranter und robust ausgelegter Softwarelösungen zur Reduzierung von Systemausfällen und Fehlfunktionen im operativen Betrieb.
- Standardmäßige Umsetzung datenschutzfreundlicher Voreinstellungen gemäß Art. 25 Abs. 2 DSGVO („Privacy by Default“), insbesondere im Hinblick auf Datenminimierung und Zugriffskontrolle.
- Vertraglich geregelte Festlegung von Art, Umfang und Turnus der vom Auftraggeber zu sichernden Daten, um eine kontinuierliche und DSGVO-konforme Datensicherung zu gewährleisten.

Augsburg, den 28.06.2025

Geprüft:

Datenschutz Serviceteam

DSGVO-KONFORM Qualifizierter Datenschutz Datenschutz - Serviceteam

Datenschutzbeauftragte:

Dipl.-Ing. Heike Lenz

Augsburg den 30.06.2025

Verantwortliche SEWOBE AG

SEWOBE

SEWOBE AG
Werner-Haas-Str. 8
D - 86153 Augsburg
Tel.: +49 821 455 564 100
Fax: +49 821 455 564 101
E-Mail: info@sewobe.de

Firmenstempel

Kaufm. Vorstand Eiko Trausch

Anlage 1

Liste der beauftragten Subunternehmer

Stand 06/2025

1. Die SEWOBE AG erklärt, dass die nachfolgenden Subauftragnehmer zur Unterstützung eingesetzt werden. Mit den Unternehmen wurde ein Vertrag zur Auftragsverarbeitung geschlossen.

	Unternehmen	Adresse
1	**IONOS SE** (Rechenzentrum / Datenspeicherung) https://cloud.ionos.de/rechenzentren	Eigendorfer Straße 57 56410 Montabaur
2	**TelemaxX Telekommunikation GmbH** (Rechenzentrum, Managed Services, Telekommunikation) https://www.telemaxx.de/rechenzentrum	Amalienbadstraße 41 Bau 61 76227 Karlsruhe Deutschland
3	**Infinigate Deutschland GmbH** (N-able Solutions ULC, ehemals acmeo) Backup & Recovery www.acmeo.eu https://infinigate.de/Technologien/	Richard-Reitzner-Allee 8 85540 Haar / München
4	**Google Ireland Limited Inc.** **Geocodierung** https://www.google.de/contact/impressum.html	Gordon House, Barrow Street Dublin 4 Irland

2. Werden neue Subunternehmer beauftragt, so verpflichtet sich der Auftragnehmer die Aktualisierungen auf der Homepage des Auftragsverarbeitungsvertrags http://www.sewobe.de/datenschutz/subunternehmer zu veröffentlichen. Der Auftragnehmer erhält hierüber eine Systemnachricht. Die Auswahl neuer Subunternehmer, darf nicht dazu führen, dass das bisherige Schutzniveau unterschritten wird.