

# Datenschutz- und Datensicherheitskonzept

## Prüfbericht 2023 / 2024

Dokumentation der Datenschutz- und Datensicherheitsmaßnahmen sowie der technischen und organisatorischen Maßnahmen (TOM) der SEWOBE AG zum Nachweis der Sicherheit der Verarbeitung personenbezogener Daten gemäß Art. 32 DSGVO i. V. m. § 9 des Vertrags zur Auftragsverarbeitung zwischen Auftraggeber und Auftragnehmer / Kunde

<b>Unternehmen / Auftragnehmer:</b>	SEWOBE AG, Werner-Haas-Str. 8, 86153 Augsburg vertreten durch die Vorstände Eiko Trausch und Thomas Weishaupt (Verantwortliche i.S.d. Art. 4 DSGVO)
<b>Prüfart:</b>	Augsburg, Geschäftssitz: Werner-Haas-Str. 8, 86153 Augsburg
<b>Prüfzeitraum:</b>	15. Mai 2023 bis 31. Mai 2024
<b>Prüfer / Koordination:</b>	Datenschutz Serviceteam Augsburg, Dipl.-Ing. Heike Lenz

### INHALT

- I. **Prüfberichtsgegenstand / Rechtsgrundlagen**
- II. **Individuelle Datenschutz- und Sicherheitsmaßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung personenbezogener Daten**
  1. Allgemeines zu Datenschutz und Datensicherheit
  2. Verzeichnis der Verarbeitungstätigkeiten / Checklisten
  3. Homeoffice- bzw. Remote-Tätigkeiten - Sicherheitsmaßnahmen
  4. Datenschutzs Schulungen und Unterweisungen der Beschäftigten
  5. Verpflichtung von Beschäftigten und Dienstleistern auf Vertraulichkeit
  6. Maßnahmen zum Einsatz lizenzierter Softwareanwendungen / Kommunikationsmedien
  7. Gesicherte Entwicklungen neuer Softwareprodukte
  8. Notfallmanagement:
    - a. Notfallplan
    - b. IT-Notfall-Handbuch – Aktualisierung aufgrund eines akuten Stromausfalls
  9. Allgemeine Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung
  10. Zertifizierungen bzw. Pflege diverser Gütesiegel
    - a. „IDW PS 880 Zertifizierung“ (GOBD-Konformität)
    - b. „Trusted Cloud Label“
    - c. „SOFTWARE MADE IN GERMANY“ und „SOFTWARE HOSTED IN GERMANY“
  11. Änderungen von Berechtigungen - Erteilung oder Entzug von Zugriffsberechtigungen (z.B. Vorstandswechsel) über Ticket oder per Nachweis aus Vereinsregister etc.
- III. **Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO i. V. m. Erwägungsgrund 78 7 Anpassungen Rechtekonzept**

**Anlage 1** Aktualisierte Liste der Unterauftragnehmer (Subunternehmer oder Dienstleister)

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

## I. Prüfberichtsgegenstand / Rechtsgrundlagen

Gemäß Vertrag zur Auftragsverarbeitung (AV-Vertrag) verpflichtet sich die SEWOBE als Auftragnehmer gegenüber dem Auftraggeber zur Erstellung eines jährlichen Prüfberichts, um den Auftraggeber (im Folgenden auch „Kunde“ genannt) bei seinen Kontrollpflichten zu unterstützen und um Rechenschaft über die Art und den Umfang der Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten abzulegen.

Der Vertrag zur Auftragsverarbeitung konkretisiert die datenschutzrechtlichen Verpflichtungen zwischen Auftraggeber und Auftragnehmer gemäß Art. 28 Abs. 3 der EU-Datenschutzgrundverordnung (DSGVO), die sich aus der Erbringung der Vertragsleistungen ergeben und findet Anwendung auf alle Tätigkeiten, die mit Vertragsleistungen des Softwaremietvertrags in Verbindung stehen und bei denen Beschäftigte des Auftragnehmers bzw. dessen Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

Der Prüfbericht 2023 / 2024 dokumentiert in **Kapitel II** individuelle Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung sowie die Sicherheit personenbezogener Daten.

**Kapitel III.** beschreibt die technischen und organisatorischen Maßnahmen der SEWOBE AG, die regelmäßig evaluiert werden und als Nachweis zur Einhaltung des Datenschutzes und der Datensicherheit gemäß Art. 32 DSGVO in Verbindung mit Erwägungsgrund im Rahmen der Auftragsverarbeitung dienen.

Dieser **Prüfbericht** wird für jeden Kunden bzw. Auftraggeber der SEWOBE AG zum Download im **Serviceportal** bereitgestellt.

## II. Individuelle Datenschutz- und Sicherheitsmaßnahmen

### 1. Datenschutz und Datensicherheit im Unternehmen / Stellung der externen Datenschutzbeauftragten

Zur Gewährleistung des Datenschutzes und der IT-Sicherheit ergreift die SEWOBE AG umfangreiche Maßnahmen, u. a. involviert das Unternehmen die externe Datenschutzbeauftragte in alle wichtigen Unternehmensprozesse.

Die Beratungen und Prüfungen der Datenschutzbeauftragten umfassen hierbei den administrativen Bereich inklusive Personalauswahl, die Softwareneuentwicklungen sowie alle IT-relevanten Maßnahmen (z. B. den Einsatz von Soft- und Hardware), um die datenschutzkonforme Verarbeitung personenbezogener Daten im Gesamtprozess sicherzustellen. Die direkte Kontaktaufnahme mit der Datenschutzbeauftragten erfolgt unter [datenschutz@sewobe.de](mailto:datenschutz@sewobe.de) und ist auch auf der Homepage unter „Datenschutzhinweise“ veröffentlicht.

### 2. Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO / Checklisten

Zur Fehlervermeidung, Prüfung und Aktualisierung wurden für alle wichtigen Verarbeitungs-tätigkeiten des Unternehmens personenbezogener Daten, Verfahrensbeschreibungen und Checklisten erstellt, die von allen Beschäftigten systematisch abzarbeiten 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 Datenschutzmanagementsystem (DSMS) im Verzeichnis (VVZ) hinterlegt.

### **3. Homeoffice- bzw. Remote-Tätigkeiten: Schulungen / Unterweisung und Sicherung von Betriebs- und Kommunikationsmittel**

Um dem Wunsch der Beschäftigten nach Homeoffice- Tätigkeiten zu entsprechen und gleichzeitig die datenschutzkonforme Verarbeitung personenbezogener Daten sicherzustellen, wird den Beschäftigten in gewissen Abständen gestattet remote zu arbeiten, jedoch unter strengen Voraussetzungen. Die entsprechende Unternehmensanweisung schreibt vor, dass kundenbezogenen Projekte im Homeoffice nicht bearbeitet werden dürfen, sondern ausschließlich reine Programmierarbeiten ohne personenbezogenen Datenbezug, z.B. Softwareverbesserungen oder -neuentwicklungen.

Um die zunehmende Bedrohung durch Cyberangriffe und die damit gestiegene reale Bedrohung für Remote- oder Homeoffice-Arbeitsplätze abzusichern, wurden während des Prüfungszeitraums die sicherheitsrelevanten Vorgaben für die datenschutzkonforme Verarbeitung personenbezogener Daten im Homeoffice evaluiert und die damit verbundenen Unternehmensanweisungen, Verträge und Sicherheitsmechanismen der SEWOBE Beschäftigten angepasst. U. a. mussten teilweise die Verträge zur Betriebsmittelnutzung mit den Beschäftigten aktualisiert werden, um die Betriebsmittel, die per Remote genutzt wurden, ohne Voranmeldung auf schädliche Inhalte prüfen und diese jederzeit auf Anforderung mit verbesserter Sicherheitssoftware ausstatten zu können.

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.

Kunden, deren Organisationen schon aufgrund des Organisationszwecks zu den „besonderen Datenkategorien“ gehören, dürfen nur ausnahmsweise und unter Sicherstellung der unmöglichen Einsichtnahme Dritter, im Homeoffice bearbeitet werden. Für diese Verarbeitungstätigkeiten mit besonderen Datenkategorien ist die Genehmigung der Geschäftsführung einzuholen. Zu den besonderen Datenkategorien gehören z. B. Religionsgemeinschaften, Parteien, Gewerkschaften, Gesundheitsdaten etc. Die Beschäftigten müssen deshalb im Antrag auf Homeoffice angeben, welche Kundenprojekte im Homeoffice bearbeitet werden sollen und benötigen hierfür eine Freigabe. Während des Prüfungszeitraums wurden jedoch im Homeoffice keine sensiblen Kundendaten verarbeitet.

### **4. Datenschutzschulungen von neuen Beschäftigten / regelmäßige Unterweisungen aller Beschäftigten / besondere Unterweisungen für Auszubildende in Lehrveranstaltungen**

Alle neuen Beschäftigten, inkl. Werkstudenten und Praktikanten, erhielten an ihrem ersten Arbeitstag eine umfassende und auch dokumentierte Datenschutzschulung, die die wichtigsten Bereiche der Verarbeitung personenbezogener Daten betreffen sowie eine „Welcome-Mappe“ mit allen bisher getroffenen Maßnahmen zum Datenschutz und Regeln zum Miteinander.

Homeoffice kann von Beschäftigten / Werkstudenten erst nach ausreichender Einarbeitungszeit erfolgt und die datenschutzkonforme Verarbeitung von personenbezogenen Daten auch im Homeoffice gewährleistet werden kann. Auszubildenden ist es per se nicht gestattet, vor Ausbildungsende im Homeoffice zu arbeiten. Aufgrund des zunehmenden Sicherheitsrisikos wurden während des Prüfungszeitraums alle Beschäftigten sowohl im Umgang mit der erforderlichen Ausrüstung der Betriebsmitteln mit regelmäßigen Updates von Firewall und Antivirenprogrammen als auch bezüglich Social Engineering Risiken unterwiesen. Die Unterweisungen umfassten auch drohender Gefahren durch Cyberangriffe mittels Phishing-Mails, Trojaner und Ransomware etc. sowie auch auf die u. U. schädliche Nutzung von betriebsfremden (Werbe-) USB-Sticks.

In Unternehmensweisungen ist festgeschrieben, dass der Download und die Verwendung nicht lizenzierter Software nicht gestattet ist und regelmäßige Updates der Sicherheitsprogramme sowie Sicherheitsvorkehrungen von Betriebsmitteln vorzunehmen sind. Das Onboarding – und Systemeinstellungsteam wurde sensibilisiert, die Betriebsmittel regelmäßig stichprobenartig zu überprüfen. Auch der Download von diversen Hilfs-Apps, die nicht dem Datenschutzniveau entsprechen, ist zu unterlassen.

Die Auszubildenden des Unternehmens erhielten im Rahmen der wöchentlichen, betrieblichen Lehrveranstaltungen, zusätzlich Datenschutzunterweisungen und Hinweise zum datenschutzkonformen Verhalten im Unternehmen. Geschult wurde u. a. der Umgang mit personenbezogenen Kunden- und Interessentendaten, insbesondere die erforderliche Authentifizierung von telefonischen Kundenanfragen oder -aufträgen. Die betreffenden Inhalte wurden praxisnah erläutert und gemeinsam mit den Auszubildenden Sicherheitsmaßnahmen zu den sicherheitsrelevanten Themen entwickelt.

## **5. Verpflichtung von Beschäftigten und Dienstleistern auf Vertraulichkeit / Vertrag zur Auftragsverarbeitung mit Sub- bzw. Unterauftragnehmern**

Beschäftigte sowie externe Dienstleister der SEWOBE AG werden in Abhängigkeit der Verträge u. a. auf Vertraulichkeit, das Fernmeldegeheimnis sowie auf die Wahrung von Geschäftsgeheimnissen verpflichtet und über strafrechtlich relevante Konsequenzen bei einem Fehlverhalten belehrt. Sämtliche Verpflichtungen haben auch Wirkung über das Ende der Beauftragung hinaus. Mit Unterauftragnehmern bzw. Subunternehmen (z.B. Rechenzentren), die im Auftrag der SEWOBE AG personenbezogene (Kunden-)Daten verarbeiten, werden Verträge zur Auftragsverarbeitung geschlossen. Die betroffenen Subunternehmen können sowohl der letzten Seite dieses Berichts entnommen werden als auch auf der Homepage unter Datenschutz/ Subunternehmen.

## **6. Maßnahmen zum Einsatz geprüfter Softwareanwendungen / Einsatz sicherer Kommunikationsmedien**

### **a. Verbindliche Unternehmensanweisungen**

Die SEWOBE AG hat mit ihren Beschäftigten Schutzmaßnahmen für viele Bereiche des Unternehmens in sogenannten Unternehmens „Unternehmensanweisungen“ vereinbart. Während des Prüfungszeitraums wurden die SEWOBE Unternehmensanweisungen zum Datenschutz und zur Datensicherheit aktualisiert und die Verwendung ausschließlich lizenzierter Software, regelmäßige Updates der Sicherheitsprogramme sowie Sicherheitsvorkehrungen von Betriebsmitteln vorgeschrieben. Betriebsmittel wurden in Zusammenarbeit der IT-Abteilung und der Datenschutzbeauftragten regelmäßig stichprobenartig kontrolliert. Die hierfür notwendigen technischen und organisatorischen Maßnahmen wurden in den entsprechenden Verarbeitungstätigkeiten / Verfahrensbeschreibungen dokumentiert und im Datenschutzmanagementsystem bzw. im Handbuch abgelegt.

### **b. Reduzierung bzw. Vermeidung von Kundenverkehr via E-Mail**

Der Empfang externer Kunden-E-Mails wurde bereits in den vergangenen Jahren in fast allen Abteilungen durch die verpflichtende Kommunikation über das Ticketsystem im Serviceportal ersetzt und dadurch externe Angriffe durch virenbehaftete E-Mail-Anhänge weitgehend ausgeschlossen. Alle eingehenden E-Mails werden auf Schadsoftware gescannt und schadhafte Anhänge isoliert.

### **c. Sichere Kommunikationsmedien**

Die SEWOBE bietet sichere Kundens Schulungen über „TeamViewer“ oder „Teams“ mit Serverstandorten in Deutschland oder Europa an, damit personenbezogene Daten von Kommunikationsanbietern mit Serverstandorten in Drittländern, weder abfließen noch mitgeschnitten werden

können. Teilweise wünschen Kunden ausdrücklich, dass Schulungen und Unterweisungen mittels unsicherer Kommunikationsanbieter (z. B. Zoom oder WebEx) aus Drittländern durchgeführt werden, die nicht das gleiche Datenschutzniveau aufweisen, wie es die EU-Datenschutz-Grundverordnung vorschreibt. Die Beschäftigten der SEWOBE sind deshalb gehalten, die entsprechenden Kunden gemäß Vertrag zur Auftragsverarbeitung auf die Gefahren nicht datenschutzkonformer Datenverarbeitungen hinzuweisen. Trotz der Hinweise auf mögliche Datenabflüsse bestehen einige Kunden weiterhin auf die Nutzung dieser kritischen Kommunikationsanbieter.

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

Die SEWOBE AG evaluiert ihr digitales Datenschutzmanagementsystem (DSMS) in regelmäßigen Abständen und hat während des Prüfzeitraums das „Verzeichnis der Verarbeitungstätigkeiten“ (VVT) um neue Verarbeitungstätigkeiten erweitert, bestehende neu bewertet und angepasst. Unter die Erweiterung fallen auch einige Neuentwicklungen wichtiger Softwarefunktionen sowie Zusatzmodule zur Optimierung der Online-Verwaltungssoftware.

Die Neu- und Weiterentwicklung von Softwarefunktionen wird von der Datenschutzbeauftragten fortlaufend begleitet und auf Datenschutzkonformität geprüft. Gemeinsam mit den Vorständen und der IT-Abteilung soll damit die Sicherheit der Software gewährleistet werden, um die Einhaltung der hohen Qualitätsstandards der SEWOBE AG als Premiumanbieter von Beginn an zu gewährleisten.

## 8. Notfallmanagement: Notfallplan / Notfallhandbuch

Die SEWOBE hat für die nachfolgenden Szenarien einen Notfallplan aufgestellt. Dieser wird regelmäßig evaluiert und dem Notfallteam sowie den Beschäftigten zusätzlich in Printausfertigung bzw. auf Speichermedien ausgehändigt, um alle Beschäftigten im Notfall gleichlautend instruieren und einen geordneten Wiederanlauf gewährleisten zu können. Der Notfallplan musste im Prüfzeitraum erneut angepasst und um Personen und Maßnahmen erweitert werden, da es zu einem akutem Stromausfall kam.

- a. **Notfallplan:** Die SEWOBE AG hat im Prüfungsbericht den Notfallplan um Maßnahmen während der Prüfungszeitraums ergänzt und evaluiert. Dies wurde notwendig aufgrund eines ca. 90 minütigen Stromausfalls in Augsburg, von dem eigene Kommunikationssysteme betroffen waren.

Der Notfallplan umfasst folgende Gefahrenfaktoren:

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

Im Fokus der v. g. Notfallszenarien steht der Schutz aller personenbezogenen Daten, die die SEWOBE verarbeitet, insbesondere Maßnahmen zur Minimierung etwaiger Ausfallszeiten und eine schnellen Wiederanlauf.

Unterschiedliche Gefahrenlagen werden unter möglichst realen Bedingungen turnus-mäßig simuliert und der Wiederanlaufplan mit allen Beschäftigten besprochen.

Im Notfallplan werden neben möglichen Gefahrenlagen, alle Unternehmensbereiche mit sämtlichen Beschäftigten inklusive deren Vertreter dokumentiert und durch regelmäßige Unterweisungen in die

Lage versetzt, sich vorschriftsgemäß zu verhalten. Angaben zu Ansprechpartnern, Büro-Ersatzstandorten sowie jeweils aktualisierte Kontaktdaten sollen einen reibungslosen Wiederanlauf gewährleisten.

Der Notfallplan wird in verschiedenen Dateiformaten vorgehalten, um auch bei etwaigen Systemausfällen Zugriff auf alle erforderlichen Kontaktdaten zu haben.

- b. IT-Notfallhandbuch:** Um z.B. nach einem Cyberangriff das System schnellstmöglich wieder hochfahren zu können, hält die Unternehmensführung die Dokumentation der erforderlichen Schritte zum Neustart des Systems in Form eines IT-Notfallhandbuchs wohl in einer Print- als auch in einer digitalen Fassung vor. Das Handbuch beinhaltet die Details zum Wiederanlauf.

Das **Notfallhandbuch** wurde nach einem Stromausfall aufgrund eines Blitzeinschlags in ein Umspannwerk um diesen Fall angepasst, da die gesamte Innenstadt am 29. Mai 2024 von Augsburg bis zu 90 Minuten ohne Strom war.

#### **Fazit – Auswirkungen Stromausfall am 29.05.2024:**

Die Schadenanalyse der SEWOBE bezüglich der Auswirkungen auf alle Systeme ergab, dass die unterbrechungsfreie Stromversorgung (USV) der SEWOBE weiter ausgebaut muss, damit auch längere Stromunterbrechungen abgesichert werden können. Der Stromausfall hatte keine Auswirkungen für Auftraggeber und Kunden.

#### **9. Allgemeine Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung**

##### **(Art. 32 Abs. 1 lit. d DSGVO und Art. 25 Abs. 1 DSGVO)**

Die SEWOBE AG hat, wie auch bereits in den Vorjahren, folgende weitere wichtige Kontrollverfahren zur Gewährleistung des Datenschutzes und der Sicherheit der Verarbeitung bei der Technikgestaltung implementiert und fortgeführt, u. a.:

- a. Konzept-Evaluierung:** Regelmäßige Aktualisierung und Fortschreibung des „Datenschutz- und IT-Sicherheitskonzepts“ jeweils unter Mitwirkung der Verantwortlichen, der betroffenen Abteilungen und der Datenschutzbeauftragten.
- b. System-Monitoring:** Einsatz von verfahrensunabhängigen „Plausibilitäts- und Sicherheitsprüfungen“ (u. a. interne Erstellung von Prüfberichten zur Sicherheit der eingesetzten Server). Das Unternehmen setzt neben einer eigens entwickelten Sicherheitssoftware, auch die umfassende Überwachungslösung von „CheckMK“ für verschiedene Arten von IT-Infrastrukturen, einschließlich Servern, Netzwerken, Anwendungen und Diensten ein. Die Systeme werden 24/7 von Monitoring-Software überwacht. Zusätzlich werden werktags von 7 Uhr bis 22 Uhr und am Wochenende und an Feiertagen, von 10 bis 17 Uhr, die Systeme von Beschäftigten im Rahmen eines Bereitschaftsdienstes beobachtet, um notfalls eingreifen zu können.
- c. Notfall-Management:** Regelmäßige Aktualisierung des Notfallplans gem. Ziffer 8 a.
- d. Zyklische Prüfung** und Aktualisierung der Softwareverträge inkl. der Verträge zur Auftragsverarbeitung, Unternehmensanweisungen und Checklisten

## 10. Zertifizierungen und Gütesiegel der SEWOBE Software Services (SoftwareMANAGER)

### 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 Wirtschaftsprüfer 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. Der erfolgreiche Abschluss der GoBD Zertifizierung erfolgte Ende Mai / Anfang Juni 2023.

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 Buchhaltungssystems fest und sorgt für nachhaltige und effiziente Prozesse in der Buchhaltung.
- Kontinuierliche Verbesserung der Buchhaltung durch regelmäßige Audit

Seit der letzten Zertifizierung im Juni 2023 wurden die geprüften Bereiche der Buchhaltung nur in geringem Maße angepasst. Eine Überprüfung der Zertifizierung ist geplant, sobald umfangreichere Optimierungen des Buchhaltungsmoduls umgesetzt werden (z. B. DATEV-Schnittstellen, weitere Kontenrahmen etc.).

*Die nachfolgenden Siegel wurden im Zeitraum 2023 / 2024 überprüft und sofern erforderlich erneuert:*

### 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 rechtskonformen 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, deutschsprachige 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>

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

Während des Prüfungszeitraums wurden erneut von Organisationen (vertraglich auch Kunde oder Kunde oder Auftraggeber genannt) mehrere Nachrichten per E-Mail oder Brief gesendet, die zum Entzug von Zugriffen bisher Berechtigten aufforderten.

Die SEWOBE ist als Auftragnehmer und gemäß Vertrag zur Auftragsverarbeitung jedoch verpflichtet, ausschließlich auf Weisung von Berechtigten zu agieren. Das bedeutet, dass die Änderung von Berechtigungen, die nicht innerhalb der Organisationssoftware bzw. im Serviceportal der SEWOBE hinterlegt wurden, ohne entsprechende Vorlage von Unterlagen nicht autorisiert werden können. Dies obliegt einzig der Verantwortung und Weisung des nachweislich berechtigten Vorstands oder Vorsitzenden der Organisation.

Zugriffsrechte können durch die SEWOBE nur dann auf Weisung erteilt werden, wenn in Schriftform ein beglaubigter Beschluss oder ein Registernachweis über die Veränderung der Berechtigten vorliegt und der Antragsteller unter Vorlage eines Identitätsnachweises bestätigt, dass er bevollmächtigt ist, diese Zugriffe anzuweisen bzw. diese Rechte ausüben zu können. In den Softwaremietvertrag wurde deshalb der Zusatz aufgenommen, dass „Wechsel von Zugriffsberechtigungen“ umgehend von der Organisation selbst in der Software zu hinterlegen sind. Die SEWOBE kann Berechtigungen ohne entsprechende Nachweise nicht beurteilen kann. Eine Kommunikation außerhalb der Schriftform oder des Kundenportals ist vertraglich ausgeschlossen.

## III. Technische und organisatorische Maßnahmen

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

### 1. Sicherheitsmaßnahmen der SEWOBE AG / SoftwareMANAGER-Lösungen

Um die Sicherheit von Kunden und Auftragnehmern zu erhöhen, hat die SEWOBE AG nachfolgende Verfahren im Unternehmen und innerhalb der Softwarelösung implementiert:

#### 1.1 Verpflichtende Nutzung des Serviceportals / Verfolgung von Verstößen gegen die E-Mail-Kommunikationsrichtlinie

Die SEWOBE AG hat ihre E-Mail-Kommunikation mit Kunden bzw. Auftraggebern aus Sicherheitsgründen eingestellt und betreibt für ihre Kunden das SEWOBE-Serviceportal, um über diesen Bereich die gesamte Kommunikation abwickeln zu können. Die Nutzung des Serviceportal ist im Softwarenutzungsvertrag verpflichtend geregelt.

#### 1.2 Das Serviceportal ermöglicht eine gesicherte Kommunikation zwischen Auftraggeber (Kunde) und Auftragnehmer (SEWOBE AG) und verfügt über einen passwortgesicherten Login. Über das Serviceportal können Services wie z. B. Support-Anfragen, Übermittlung von sensiblen Daten oder das Dokumentenarchiv bereitgestellt werden. Der Auftraggeber bzw. die bevollmächtigten Nutzer werden vertraglich dazu verpflichtet, das Serviceportal zu nutzen und aufgefordert, keine sensiblen Daten per E-Mail zu senden.

Obwohl sich diese Maßnahme seit Jahren bewährt hat, haben etliche Kunden während des Prüfungszeitraums und entgegen vertraglichen Vereinbarungen, erneut sensible Daten per E-Mail an den Auftragnehmer gesendet. Wiederkehrende Hinweise auf diese Verstöße blieben teilweise un-



beachtet, weshalb sich die SEWOBE AG verstärkt an die Verantwortlichen oder die Datenschutzbeauftragten der betroffenen Kunden mit entsprechenden Hinweisen wenden musste. Diese Praxis wird auch zukünftig bei Verstößen fortgeführt werden.

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-Authentifizierung 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 Multifaktorauthentifizierung und Passwort gesichert.

### **1.4 Sicherheitsaspekt „Mitgliederportal“**

Das in der „Pro“ und Pro *Plus* Version erhältliche Mitglieder- bzw. Kundenportal gewährleistet eine sichere Kommunikation innerhalb der Kunden-Organisationen der Auftraggeber. Im Mitglieder- bzw. Kundenportal können sämtliche Informationen für Mitglieder bzw. Bevollmächtigte im gesicherten Bereich zum Download hinterlegt werden, ohne dass diese hinterlegten Dateien, die meist einen Personenbezug aufweisen, per E-Mail versendet werden müssen.

## **2. Vertraulichkeit**

Vermeidung von unbefugter Informationsgewinnung durch Sicherheitsmaßnahmen, die unberechtigte Zugriffe auf gespeicherte bzw. auf übermittelte personenbezogene Daten verhindern.

### **2.1. Zutrittskontrolle**

Folgende Maßnahmen trifft die SEWOBE AG an ihrem Geschäftssitz, um Unbefugten den räumlichen Zutritt zu solchen Datenverarbeitungsanlagen zu verwehren, mittels derer personenbezogene Daten verarbeitet oder genutzt werden:

- Elektronische Zutrittserfassung: Abschlusstürsicherung mit Zutrittsregelung, die zusätzlich kameraüberwacht ist, d.h. Beschäftigte der SEWOBE AG erhalten über ein elektronisches Schließsystem Zutritt zu den allgemeinen Geschäftsräumen. Deren Daten werden protokolliert und in regelmäßigen Abständen wieder gelöscht. Mit dem Hersteller wurde ein AV-Vertrag geschlossen.
- Betriebsfremde haben keinen Zutritt zu den Unternehmensräumen und werden persönlich vom Frontoffice in Empfang genommen und überprüft, d. h. Besucher bzw. Dritte erhalten nur Zutritt zu den Geschäftsräumen der SEWOBE AG nach vorheriger Anmeldung und können sich auch innerhalb der Geschäftsräume nicht frei bewegen.
- Einsatz zusätzlicher elektronischer Sicherheitsschlösser in allen Räumen mit sensibler Infrastruktur, z.B. erhält nur eng begrenzter Personenkreis Zugang zum Serverraum. Der Zutritt wird ebenfalls protokolliert.
- Es liegen schriftliche Festlegungen zur Raumnutzung für Beschäftigte sowie sonstige befugte Personen sowie Dienstleister und Besucher vor.
- Kameraüberwachung umfasst folgende Räumlichkeiten: Büroabschlusstür, Entrée, Flure, sowie Räume mit sensibler Infrastruktur

### **2.2. Zugangskontrolle**

Der Zugang zu Datenstationen (PC, Server, Netzkomponenten) erfolgt durch Zugriffsberechtigungsvergabe und Authentifizierung in allen Systemen. Die Zugangsregelungen werden mit der Prämisse eingesetzt, den Zugang zu Datenverarbeitungssystemen für Unbefugte zu verhindern und umfassen

folgende Maßnahmen:

- Authentifizierung mit Benutzername / Passwort
- Verpflichtende zusätzliche Zwei-Faktor-Authentifizierung
- Komplexität der Passwörter: Passwortvergabe (Klein- und Großbuchstaben, Sonderzeichen, Zahlen, mindestens 8 Zeichen)
- Definierte Wechselfristen, Passworthistorie.
- Beschränkte Anzahl von Fehleingaben
- Rechtekonzept: Rechtezuweisungen sind an Zugangskennungen gebunden
- Zuordnung einzelner Terminals
- Bildschirmsperre bei Abwesenheit mit jeweiliger Passwort-Aktivierung
- Einsatz von VPN-Technologien
- Prüf-, Abstimm- und Kontrollsysteme

### 2.3. Zugriffskontrolle

Maßnahmen zur Verhinderung von unerlaubten Tätigkeiten (z.B. unbefugtes Lesen, Kopieren, Verändern oder Entfernen) in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen:

- Die SoftwareMANAGER der SEWOBE AG beinhalten ein Berechtigungskonzept und ermöglichen die Erstellung von Benutzerprofilen / Regelung der Zugriffsberechtigung, diese sind mittels Historie nachprüfbar.
- Firewall und Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches sind im Einsatz.
- VPN-Verbindung auf allen mobilen Endgeräten (VPN)
- Festplattenverschlüsselung auf allen mobilen Endgeräten
- Beschränkung der Administratorrechte auf das Notwendigste / Überwachung durch techn. Vorstand
- Eng begrenzte Zugriffsberechtigung auf Datenbestände und Funktionen (Rechtekonzepte)
- Arbeitsanweisungen und Bearbeitungsverfahren für Datenverarbeitungsvorlagen
- Gesicherte Nutzung von USB-Schnittstellen
- Verschlüsselung von (mobilen) Datenträgern
- Protokollierung von Zugriffen auf Anwendungen
- Sichere Aufbewahrung von Datenträgern
- Kontrollierte physische Vernichtung von Datenträgern durch zertifizierte Unternehmen (Zertifikate z.B. von Documentus Bayern / Reisswolf)
- Regelmäßige Überprüfung der Clear Desk Policy

### 2.4. Trennungskontrolle

Maßnahmen zur Gewährleistung der Trennung von Daten, die zu unterschiedlichen Zwecken verarbeitet werden:

- Physikalische getrennte Speicherung auf gesonderten Systemen, u. a. Einsatz mehrerer Server für unterschiedliche Mandanten, separate Aufbewahrung der Backups an weiteren Standorten etc.
- Tabellarische Mandantentrennung sowie Trennung von Daten verschiedener Auftraggeber / Mandanten
- Datenbankrechte - Zuordnung durch Geschäftsleitung oder technischen Vorstand
- Trennung von Test- und Live-Umgebungen

### 2.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in der Weise, dass der Personen bezug von Daten nicht vollständig hergestellt werden kann, z. B. durch Zuweisung von Kunden- bzw. Mitgliedsnummern.

## 2.6. 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:

- SSL/TSL Verschlüsselungszertifikate
- Kommunikation über das SEWOBE Serviceportal bzw. über ein Ticketsystem zur Vermeidung von Kommunikations- bzw. von Datenübertragungen via E-Mail, USB oder sonstige Datenträger.
- Implementierung eines Bewerberportals zur sicheren Übermittlung von sensiblen Beschäftigtendaten.

## 3. Integrität / Authentizität

Maßnahmen zur Gewährleistung der Korrektheit, Unveränderbarkeit und Verlässlichkeit von Daten und Systemen sowie Maßnahmen zur Vermeidung von fehlerhaften Ergebnissen durch Soft- und Hardware.

### 3.1. Weitergabekontrolle

Maßnahmen zur Vermeidung von unbefugtem Lesen, Kopieren, Veränderung oder Verlust während des Transports oder der Speicherung bzw. der Überprüfung bzw. Feststellung der jeweiligen Empfänger:

- Versand wichtiger Dokumente mit personenbezogenem Inhalt (z.B. Verträge) vorzugsweise postalisch oder über SEWOBE Serviceportal - Einsatz von Standleitungen bzw. VPN-Verbindungen
- Einsatz von Firewall und Virenschutz – Aktualisierung von Sicherheitssoftware
- Dokumentation der Empfänger von Daten unter Angabe der Zweckgebundenheit und Löschfrist (z.B. im Verarbeitungsverzeichnis).
- Protokollierung der Übermittlung / Identitätsprüfung der Empfänger
- Dokumentation und stete Aktualisierung der Hard- und Software über ein Inventar-Modul.
- Im Ausnahmefall: E-Mail-Verschlüsselung via ZIP-Datei (regulär erfolgt jedoch die Abwicklung über das SEWOBE Serviceportal und nur auf ausdrücklichen Wunsch außerhalb des Portals)
- Entsorgung von Festplatten, Disketten und Akten durch zertifizierte Unternehmen und entsprechende Nachweise
- Unterweisung der Beschäftigten bezgl. der rein zweckgebundenen Verarbeitung
- Kein Einsatz mobiler Datenträger wie USB-Sticks oder externe Festplatten

### 3.2. Eingabekontrolle / Verarbeitungskontrolle

Maßnahmen zur Gewährleistung der Überprüfung und Feststellung, welche Benutzer bzw. Beschäftigten die Daten eingegeben, verändert oder gelöscht haben:

- Checkliste zur Vergabe von Zugangsregelungen und Benutzungsberechtigungen zum SEWOBE SoftwareMANAGER
- Automatisierte Dokumentation der jeweiligen Verarbeitungsschritte innerhalb der SEWOBE Software „Historie“.
- Protokollierung aller Verarbeitungsschritte in der Historie: z. B. Feststellung des individuellen Benutzers, ebenso Uhrzeit und Länge etc.
- Möglichkeit zur Erstellung individueller Auswertungen bzw. Protokolle innerhalb der SEWOBE Software zu jeglichen Verarbeitungsschritten.
- Integrierte Scanfunktion / Uploader zur Fehlervermeidung und zum Schutz vor Manipulation von Daten

### 3.3. Dokumentationskontrolle

Maßnahmen zur Sicherung der nachvollziehbaren Verfahrensweisen bei der Verarbeitung personenbezogener Daten:

- Führung eines Verzeichnisses über alle relevanten Verarbeitungstätigkeiten (VVT) innerhalb des Datenschutzmanagementsystems (DSMS), d.h. Dokumentation aller relevanten Verarbeitungstätigkeiten.
- Dokumentation der zulässigen Arten des Datentransfers
- Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration sowie personalisierte Zuordnungen.

### 3.4. Auftragskontrolle

Gewährleistung der Verarbeitung von personenbezogenen Daten durch den Auftragnehmer:

- Jegliche Aktivität der Auftragnehmers basiert auf einem Vertrag zur Auftragsverarbeitung bzw. auf Basis eines Auftrages und erfolgt ausschließlich auf Weisung des Auftraggebers
- Mündliche Aufträge sind umgehend schriftlich zu bestätigen
- Vor Auftragsübernahme erfolgt die Prüfung der Berechtigung des Auftraggebers; berechnete Personen sind im Vertrag und in der SEWOBE Softwarelösung hinterlegt.
- Formalisierung der Auftragserteilung innerhalb des SEWOBE Ticketsystems, d. h. Auftragsausführung erfolgt erst nach Freigabe durch den berechtigten Auftraggeber
- Regelungen zur Fernwartung via TeamViewer oder Teams (mit Servern in Deutschland bzw. Europa)
- Regelung zulässiger Kommunikationsmedien in Abhängigkeit von Serverstandorten in der EU
- Verpflichtende Datenschutzmaßnahmen beider Parteien in mindestens gleichem Umfang

## 4. Verfügbarkeit und Belastbarkeit

Maßnahmen zur Gewährleistung des Schutzes bzw. der Belastbarkeit personenbezogener Daten und IT-Systeme gegen (zufällige) Zerstörung, Unterbrechung oder Verlust

### 4.1. Verfügbarkeitskontrolle

- Unterbrechungsfrei Stromversorgung (USV-Anlagen) / Überspannungsschutz  
Überarbeitung der Systeme nach Stromausfall Ende Mai 2024
- Klimaanlage im Serverraum inkl. Online-Überwachung von Temperatur und Feuchtigkeitsmessung im Serverraum
- Schutzsteckdosen im Serverraum
- Feuerlöschgeräte an mehreren Stellen in den Räumen der SEWOBE AG
- Feuer- und Rauchmelder
- Regelmäßige Backup-Lösungen an unterschiedlichen Standorten
- Kameraüberwachung der Infrastruktur
- Firewall und Virenschutz
- Regelmäßige Evaluierung und Aktualisierung des Notfallkonzepts -> Wiederanlaufplan
- Verträge zur Auftragsverarbeitung mit den Betreibern der Rechenzentren

### 4.2. Belastbarkeit (Widerstandsfähigkeit von Systemen und Dienstleistungen)

Maßnahmen zur Gewährleistung der Aufrechterhaltung von technischen Systemen bei Störung bzw. Teilausfällen:

- Schutz vor Überlastung / Durchführung von Penetrationstests
- Redundante Systemauslegung
- Ausfallsicherheits-/Hochverfügbarkeitskonzept

- Einsatz fehlerintoleranter Software
- Datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DSGVO
- Vertragliche Regelung zu Art und Umfang der vom Auftraggeber erfassten Daten zur regelmäßigen Sicherung

Augsburg, den 18.06.2024

**Geprüft:**



**Datenschutzbeauftragte:**

Dipl.-Ing. Heike Lenz

Augsburg den 26.06.2024

**Verantwortliche SEWOBE AG**



Firmenstempel

Kaufm. Vorstand Eiko Trausch

## Liste der beauftragten Subunternehmer

Stand 06/2024

- Die SEWOBE AG erklärt, dass die nachfolgenden Subauftragnehmer zur Unterstützung beim Hosting eingesetzt werden.

	Firma	Adresse
1	<b>IONOS SE</b> (Rechenzentrum / Datenspeicherung) <a href="https://cloud.ionos.de/rechenzentren">https://cloud.ionos.de/rechenzentren</a>	Eigendorfer Straße 57 56410 Montabaur
2	<b>TelemaxX Telekommunikation GmbH</b> (Rechenzentrum, Managed Services, Telekommunikation) <a href="https://www.telemaxx.de/rechenzentrum">https://www.telemaxx.de/rechenzentrum</a>	Amalienbadstraße 41 Bau 61 76227 Karlsruhe Deutschland
3	<b>Infinigate Deutschland GmbH</b> (Business Unit mit acmeo) Backup & Recovery <a href="http://www.acmeo.eu">www.acmeo.eu</a> <a href="https://infinigate.de/Technologien/">https://infinigate.de/Technologien/</a>	Richard-Reitzner-Allee 8 85540 Haar / München

- Werden neue Subunternehmer beauftragt, so verpflichtet sich der Auftragnehmer die Aktualisierungen auf der Website gem. § 7 Abs. 5 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.

**Hinweis zu Veränderungen:** Seit Einführung der DSGVO und der erforderlichen Veröffentlichung der Dienstleister bzw. Subunternehmen gab es keine Veränderung bei der Zusammenarbeit. Geändert haben sich jedoch Firmierungen durch Kooperationen der Subunternehmen.