# Prüfbericht 2021 / 2022

Technische und organisatorische Maßnahmen 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 / Kunde und Auftragnehmer

| | |
|---|---|
| **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:** | Unternehmenssitz: Werner-Haas-Str. 8, 86153 Augsburg sowie die Zweigniederlassungen |
| **Prüfer:** | Datenschutz Serviceteam Augsburg, Koordination Dipl.-Ing. Heike Lenz |
| **Prüfzeitraum:** | Mai 2021 bis Mai 2022 |
| **Ausfertigungsdatum:** | 26.05.2022 |

## INHALT



---

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

# I. Prüfberichtsgegenstand

Gemäß § 9 des Vertrags zur Auftragsverarbeitung verpflichtet sich die SEWOBE AG als Auftragnehmer, einen jährlichen Prüfbericht zu erstellen, um Auftraggeber bzw. Kunden bei ihren Kontrollpflichten zu unterstützen und um Rechenschaft über den Umfang der Sicherheitsmaßnamen bei der Verarbeitung personenbezogener Daten abzulegen.

Der Prüfbericht 2021 / 2022 dokumentiert in den **Kapiteln II.** und **III.** die individuellen organisatorischen Maßnahmen und deren Rechtmäßigkeit sowie die Sicherheit bei der Verarbeitung personenbezogener Daten. Kapitel II dokumentiert die erweiterten Schutzmaßnahmen durch anteilige Remote-Tätigkeiten während der Pandemie.

**Kapitel IV.** beschreibt die allgemeinen technischen und organisatorischen Maßnahmen der SEWOBE AG, die regelmäßig evaluiert werden und als Nachweis der Einhaltung des Datenschutzes und der Datensicherheit gemäß Art. 32 DSGVO im Rahmen der Auftragsverarbeitung dienen.

# II. Besondere Datenschutzmaßnahmen während der Pandemielage

### 1. Sicherheitsmaßnahmen: Kunden und Beschäftigte / Schulungsmaßnahmen

Zum Schutz der Beschäftigten und Auftraggeber / Kunden wurden im Prüfungszeitraum die Hygienevorschriften regelmäßig überprüft und angepasst und deshalb von Kundenbesuchen Abstand genommen.
Die Datenschutzschulungen der Beschäftigten wurden vorwiegend im Digitalformat in Einzelschulungen oder in Kleingruppen veranstaltet, wenn möglich im Unternehmen und am Arbeitsplatz, sofern die geltenden Hygienemaßnahmen eingehalten werden konnten.
Kundenschulungen und Supportmaßnahmen fanden deshalb über die Kommunikationsmedien *TeamViewer* oder *MS-Teams* statt, deren Serverstandorte sich in Deutschland oder in der Europäischen Union befinden.

Teilweise mussten auf ausdrückliche Weisung einiger Auftraggeber, Schulungen über Kommunikationsanbieter (z. B. Zoom) aus Drittländern durchgeführt werden. Die Beschäftigten der SEWOBE AG haben auf die Gefahren nicht DSGVO-konformer Kommunikationsmedien mit Serverstandorten in Drittländern in Verbindung mit einem möglichen Datenabfluss hingewiesen.
Obwohl diese Gefahr nicht ausgeschlossen werden konnte, bestanden einige Auftragnehmer auf die Nutzung kritischer Kommunikationsmedien.

## 2. Datenschutzschulungen der Beschäftigte / verstärkte Cyberangriffe

Ein weiterer Schwerpunkt während des Prüfungszeitraums bildete die Sensibilisierung der Beschäftigten zur Vermeidung gezielter Angriffe auf Hard- und Software bzw. Social-Engineering im Homeoffice.

Die Beschäftigten wurden aufgrund des erhöhten Sicherheitsrisikos regelmäßig sowohl im Umgang mit der erforderlichen Ausrüstung und der notwendigen Überprüfung der Hardware trainiert als auch regelmäßig in der datenschutzkonformen Verarbeitung personenbezogener Daten unterwiesen. Insbesondere auf die erforderliche Vermeidung drohender Gefahren durch Cyberangriffe mittels Phishing-Mails, Trojaner und Ransomware etc., sowie auch auf die ggf. schädliche Nutzung von betriebsfremden (Werbe-) USB-Sticks wurde aufmerksam gemacht.
Ebenso wurde die Verwendung ausschließlich lizensierter Software, regelmäßige Updates der Sicherheitsprogramme sowie Sicherheitsvorkehrungen von PCs vorgeschrieben und von der IT-Abteilung und der Datenschutzbeauftragten immer wieder stichprobenartig kontrolliert. Die hierfür notwendigen technischen und organisatorischen Maßnahmen wurden in den entsprechenden Verarbeitungstätigkeiten (Verfahrensbeschreibungen) dokumentiert und im Datenschutzmanagementsystem bzw. in den jeweiligen Fachbereichen des Handbuchs abgelegt.

Die Auszubildenden des Unternehmens erhielten im Rahmen der betrieblichen Lehrveranstaltungen zusätzlich wöchentliche Datenschutzunterweisungen und Sicherheitshinweise zum Verhalten im Unternehmen. Diese betrafen den Umgang mit u.a. personenbezogenen Kunden- und Interessentendaten, E-Mail-Anfragen und Kundenanrufen. Die betreffenden datenschutzrechtlichen Inhalte wurden praxisnah erläutert und gemeinsame Sicherheitsmaßnahmen mit den Auszubildenden entwickelt.

## 3. Anpassung der Homeoffice-Regularien und Vorgaben zu Remote-Tätigkeiten / Ausstattung von Betriebsmitteln

Aufgrund der vermehrten Cyberangriffe und der gestiegenen realen Bedrohung durch ungeschützte Remote- oder Homeoffice-Arbeitsplätze, wurden während des Prüfungszeitraums, die sicherheitsrelevanten Vorgaben für die datenschutzkonforme Verarbeitung personenbezogener Daten evaluiert und die Unternehmens- bzw. Arbeitsanweisungen der SEWOBE AG angepasst. U. a. mussten die Betriebsmittelvereinbarungen mit den Beschäftigten aktualisiert werden, um z.B. die Betriebsmittel, die per Remote genutzt wurden, auch im Homeoffice überprüfen zu können und diese mit aktueller Sicherheitssoftware auszustatten. Im Homeoffice durfte nur über eine VPN (Virtual Private Network) Anbindung gearbeitet werden.

Die gesetzlichen Vorgaben des Infektionsschutzgesetzes und des damit einhergehenden

verpflichtenden Angebots von Homeoffice-Arbeitsplätzen, machten erweiterte Risikoanalyse der Kundendaten erforderlich. Die hierausfolgende Bedingung *„, wenn keine zwingenden betriebsbedingten Gründe entgegenstehen"*, erforderte eine Überprüfung der betroffenen Datenkategorien.
Im Ergebnis wurde festgestellt, dass das Unternehmen überdurchschnittlich viele „besondere Datenkategorien" von Auftragnehmern / Kunden verarbeitet. Zu diesen Daten gehören z.B. Religionsangehörigkeit, sexuelle Orientierung, politische Überzeugungen, Gesundheitsdaten, sowie Weltanschauung etc. Aus diesem Grund wurde festgelegt, dass im Homeoffice ausschließlich nur personenbezogenen Kundendaten verarbeitet werden dürfen, die nicht unter die besonderen Datenkategorien fallen und von denen kein erhöhtes Risiko für diesen Personenkreis ausgeht.
Somit beschränkt sich eine Tätigkeit im Homeoffice für die Beschäftigten der SEWOBE AG auf die reine Programmierung bzw. auf die Ticketbearbeitung, die keinen Bezug zu besonderen Datenkategorien aufweisen.

**FAZIT zu Datenschutzverletzungen:** Während des Prüfungszeitraums konnten keine erfolgreichen Angriffe auf Servern der SEWOBE oder der beauftragten Dienstleister gemäß Anlage festgestellt werden. Auch Datenschutzverstöße durch Beschäftigte konnten nicht festgestellt werden.

## III. Individuelle organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit

### 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 von Beginn an die externe Datenschutzbeauftragte in alle wichtigen Unternehmensprozesse und -entwicklungen. Die Beratungen und Prüfungen der Datenschutzbeauftragten umfassen hierbei den unternehmerischen Verwaltungsbereich, die Softwareneuentwicklungen sowie alle IT-relevanten Maßnahmen (z.B. den Einsatz von Soft- und Hardware), um die datenschutzkonforme Verarbeitung personenbezogener Daten im Gesamtprozess sicher zu stellen. Kontaktdaten: datenschutz@sewobe.de.

### 2. Sicherheit der Verarbeitung personenbezogener Daten

Zur Fehlervermeidung wurden für alle wichtigen Verarbeitungstätigkeiten personenbezogener Daten Checklisten und Verfahrensbeschreibungen erstellt, die von allen Beschäftigten systematisch abzuarbeiten und vor Abschluss eines Projektes vorzulegen sind, d.h. dass ein

Vorgang erst nach Dokumentation aller hierfür notwendigen Vorgaben abgeschlossen werden darf. Alle erforderlichen Verarbeitungstätigkeiten werden im Datenschutzmanagement-system (DSMS) hinterlegt

## 3. Datenschutzmanagementsystem (DSMS) / Neuentwicklungen 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 relevante Verarbeitungstätigkeiten erweitert und bestehende neu bewertet und ggf. angepasst. Unter die Erweiterung fallen auch viele Neuentwicklungen wichtiger Softwarefunktionen sowie Zusatzmodule zur Optimierung der Verwaltungs-software. Diese wurden während der Entwicklung von der Datenschutzbeauftragten fortlaufend begleitet, um die Einhaltung der hohen Qualitätsstandards der SEWOBE AG (u.a. Datensparsamkeit und Transparenz) von Beginn an zu gewährleisten.

## 4. Allgemeine Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO und Art. 25 Abs. 1 DSGVO)

Die SEWOBE AG hat, wie schon im vergangenen Jahr, folgende wichtige Kontrollverfahren zur Gewährleistung des Datenschutzes und der Sicherheit der Verarbeitung bei der Technikgestaltung implementiert und fortgeführt, z.B.:

- Regelmäßige Aktualisierung und Fortschreibung des Datenschutz- und IT-Sicherheitskonzeptes unter Mitwirkung der Verantwortlichen, der betroffenen Abteilungen sowie der Datenschutzbeauftragten.
- Einsatz von verfahrensunabhängigen Plausibilitäts- und Sicherheitsprüfungen (u.a. interne Erstellung von Prüfberichten zur Sicherheit der eingesetzten Server).

## 5. Verpflichtung von Beschäftigten (Mitarbeiter, Praktikanten etc.) und Dienstleistern auf Vertraulichkeit / Vertrag zur Auftragsverarbeitung mit Sub- bzw. Unterauftragnehmern

Beschäftigte aller Art sowie externe Dienstleister der SEWOBE AG werden auf Vertraulichkeit, das Fernmeldegeheimnis, auf die Wahrung von Geschäftsgeheimnissen u.v.m. verpflichtet und über arbeits- und strafrechtliche Konsequenzen bei einem Fehlverhalten belehrt. Sämtliche Vertraulichkeitsverpflichtungen haben auch Wirkung über das Ende der Tätigkeit der Beschäftigten hinaus. Mit Unterauftragnehmer bzw. Subunternehmern (z.B. Rechenzentren), die im Auftrag der SEWOBE AG personenbezogene (Kunden-)Daten verarbeiten, werden Verträge zur Auftragsverarbeitung geschlossen. Die betroffenen Unternehmen können der letzten Seite dieses Berichts entnommen werden und sind auch auf der Homepage unter Datenschutz / Subunternehmen veröffentlicht.

**6. Gütesiegel bzw. Zertifizierungen der SEWOBE Software Services** (SoftwareMANAGER)

Sämtliche Siegel wurden im Zeitraum 2021 / 2022 überprüft und sofern erforderlich erneuert.

- **„Trusted Cloud e.V."**

  Die SEWOBE AG hat sich mit ihren Services (SoftwareMANAGER) wiederholt erfolgreich überprüfen lassen. Hierbei handelt es sich um einen zertifizierten Service des Bundesministeriums für Wirtschaft und Energie in Zusammenarbeit mit dem Kompetenznetzwerk Trusted Cloud e. V. Im Vordergrund der Aktivitäten 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 Informationen finden Sie hierzu auf der Website: https://www.sewobe.de/news/detail/post/detail/News/trusted-cloud-label-fuer-sewobe-online-vereinssoftware/

- **„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.) unter der Schirmherrschaft des Bundesministeriums für Wirtschaft und Energie. 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. https://www.software-made-in-germany.org

# IV. 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 Software 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 aus Sicherheitsgründen eingestellt und betreibt für ihre Kunden das SEWOBE-Serviceportal, um über diesen Bereich die gesamte Kommunikation abwickeln zu können.
Das Serviceportal ermöglicht eine gesicherte Kommunikation zwischen Auftraggeber und Auftragnehmer 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 sensible Daten per E-Mail an den Auftragnehmer gesendet. Wiederkehrende Hinweise auf diese Verstöße blieben teilweise unbeachtet, 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.

### 1.2 SoftwareMANAGER: Newsletter-Versand bzw. E-Mail-Kommunikation

Während im Zeitraum 2020 / 2021 das Double Opt-in Verfahren nur zögerlich genutzt wurde, fand während des aktuellen Prüfzeitraums der automatisierte Einsatz dieser Option ohne Beanstandung und flächendeckend statt. 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.

### 1.3 Sicherheitsaspekt Mitgliederportal

Das in der „Pro" und Pro *Plus* Version erhältliche *Mitglieder- bzw. Kundenportal* gewährleistet eine sichere Kommunikation innerhalb der Auftraggeber-Organisationen. Im Mitglieder- bzw. Kundenportal können sämtliche Informationen für Mitglieder bzw. Bevollmächtigte im gesicherten Bereich zum Download hinterlegt werden, ohne dass diese 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 Empfang erfasst und überprüft, d.h. Besucher bzw. Dritte erhalten nur Zutritt zu den Geschäftsräumen der SEWOBE AG nach vorheriger Anmeldung und können sich 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, sonstige befugte Personen und Besucher vor.
- Kameraüberwachung (Abschlusstür, Flur, Räume mit sensibler Infrastruktur)

### 2.2. Zugangskontrolle

Der Zugang zu Datenstationen (PC, Server, Netzkomponenten) erfolgt durch Berechtigungsvergabe und Authentifizierung in allen Systemen. Die Zugangsregelungen werden mit der Prämisse eingesetzt, den Zugang zu Datenverarbeitungs-systemen 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, min. 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 technischen 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 verarbeiten werden:

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

### 2.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in der Weise, dass der Personenbezug 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 unbefugter Dritter nicht möglich ist:

- SSL/TSL Verschlüsselungszertifikate

- Kommunikation über ein Serviceportal bzw. über ein Ticketsystem zur Vermeidung von Kommunikation bzw. von Datenübertragungen via E-Mail, USB oder sonstige Datenträger.
- Implementierung eines Bewerberportals zur sicheren Übermittlung von sensiblen Daten.

## 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
- 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 –> nur zweckgebundene Verarbeitung
- Kein Einsatz mobiler Datenträger

### 3.2. Eingabekontrolle / Verarbeitungskontrolle

Maßnahmen zur Gewährleistung der Überprüfung und Feststellung, welche Benutzer bzw. Beschäftigte den Datenbestand eingegeben, verändert oder gelöscht haben:

- 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 personifizierte Zuordnungen.

### 3.4. Auftragskontrolle

Gewährleistung der Verarbeitung von personenbezogenen Daten durch den Auftragnehmer:

- Jegliche Aktivität der Auftragsnehmers 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; berechtigte Personen sind im Vertrag und in der SEWOBE Softwarelösung hinterlegt.
- Formalisierung der Auftragserteilung innerhalb des SEWOBE Ticketsystems, d.h. Auftragsausführung erst nach Freigabe durch den berechtigten Auftraggeber
- Regelungen zur Fernwartung via TeamViewer
- Regelung zulässiger Kommunikationsmedien
- Verpflichtende Datenschutzmaßnahmen beider Parteien in mindestens gleichem Umfang

## 4. Verfügbarkeit und Belastbarkeit

### 4.1. Verfügbarkeitskontrolle

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

- Unterbrechungsfrei Stromversorgung (USV Anlagen) / Überspannungsschutz
- 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 fehlertoleranter Software
- Datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DSGVO
- Vertragliche Regelung zu Art und Umfang der vom Auftraggeber erfassten Daten zur regelmäßigen Sicherung

| | |
|---|---|
| **Geprüft:** | Augsburg, den 26.05.2022 |
| | **Datenschutzbeauftragte:** |
| DSGVO-KONFORM Qualifizierter Datenschutz Datenschutz - Serviceteam | Dipl.-Ing. Heike Lenz Datenschutz Serviceteam |
| **Verantwortliche Vorstände SEWOBE AG** | Augsburg den 26.05.2022 |
| 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 | |
| Techn. Vorstand Thomas Weishaupt | Kaufm. Vorstand Eiko Trausch |

Anlage 1

## Liste der beauftragten Subunternehmer

Stand 05/2022

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

| | Firma | Adresse |
|---|---|---|
| 1 | **1&1 IONOS Cloud GmbH**<br><br>(Rechenzentrum / Datenspeicherung) | Eigendorfer Straße 57<br>56410 Montabaur |
| 2 | **TelemaxX Telekommunikation GmbH**<br><br>(Rechenzentrum, Managed Services, Telekommunikation) | Amalienbadstraße 41<br>Bau 61<br>76227 Karlsruhe<br>Deutschland |
| 3 | **Infinigate Deutschland GmbH**<br><br>(Business Unit mit acmeo)<br>Backup & Recovery | Richard-Reitzner-Allee 8<br>85540 Haar / München<br>www.acmeo.eu |

2. 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.