Datenschutz- und Datensicherheitskonzept 2023

Dokumentation der Datenschutz- und Datensicherheitsmaßnahmen 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:	Augsburg, Geschäftssitz
Prüfer / Koordination:	Datenschutz Serviceteam Augsburg, Dipl.-Ing. Heike Lenz

INHALT

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

I. Prüfberichtsgegenstand / Rechtsgrundlagen

Gemäß des mit jedem Kunden vereinbarten Vertrags zur Auftragsverarbeitung (AV-Vertrag) verpflichtet sich die SEWOBE als Auftragnehmer zur Erstellung eines jährlichen Prüfberichts, um die Auftraggeber (im Folgenden auch „Kunde" genannt) bei ihren Kontrollpflichten zu unterstützen und um Rechenschaft über die Art und den Umfang der Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten abzulegen.
Im
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 dem Vertragsleistungen in Verbindung stehen und bei denen Beschäftigte des Auftragnehmers bzw. dessen Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

Der Prüfbericht 2022 / 2023 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 der 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 zum Download im Kundenportal 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 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 sicherzustellen. Die direkte Kontaktaufnahme mit der Datenschutzbeauftragten erfolgt unter „datenschutz@sewobe.de" und ist auch auf der Homepage veröffentlicht.

2. Verzeichnis der Verarbeitungstätigkeiten / Checklisten

Zur Fehlervermeidung wurden für alle wichtigen Verarbeitungstätigkeiten personenbezogener Daten Verfahrensbeschreibungen und Checklisten erstellt, die von allen Beschäftigten systema-

tisch abzuarbeiten und 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) hinterlegt.

3. Homeoffice- bzw. Remote-Tätigkeiten: Anlassbezogene Schulungen / Sicherung von Betriebs- und Kommunikationsmittel

Aufgrund vermehrter Infektionserkrankungen im Unternehmen wurde zum Schutz der Beschäftigten und Kunden die Hygienevorschriften permanent an neue Situationen angepasst und vermehrt Homeoffice angeordnet.
Um die immer mehr zunehmende Bedrohung durch Cyberangriffe und die damit gestiegene reale Bedrohung für nicht ausreichend geschützte Remote- oder Homeoffice-Arbeitsplätze abzusichern, wurden während des Prüfungszeitraums die sicherheitsrelevanten Vorgaben für die datenschutzkonforme Verarbeitung personenbezogener Daten regelmäßig evaluiert und die damit verbundenen Unternehmensanweisungen, Verträge und Sicherheitsmechanismen der SEWOBE angepasst. U. a. mussten die Betriebsmittelvereinbarungen mit den Beschäftigten aktualisiert werden, um z. B. die Betriebsmittel, die per Remote genutzt wurden, ohne Voranmeldung überprüfen zu können und diese jederzeit auf Anforderung mit verbesserter Sicherheitssoftware auszustatten. Beschäftigte im Homeoffice haben zu den erhöhten Gefahren im Homeoffice anlassbezogene Schulungen mit besonderen Hinweisen zu regelmäßigen internen Sicherheitsprüfungen aller eingesetzten Betriebsmittel auf mögliche Bedrohungen durch verstärkte Cyberangriffe erhalten. 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 unter bestimmten Umständen und unter Sicherstellung der unmöglichen Einsichtnahme Dritter, im Homeoffice bearbeitet werden. Zu den besonderen Datenkategorien gehören z. B. Religionsgemeinschaften, Parteien, Gewerkschaften, Gesundheitsdaten (u.a. Selbsthilfegruppen) etc. Die Beschäftigten müssen im Antrag auf Homeoffice angegeben, welche Kundenprojekte im Homeoffice bearbeitet werden sollen und sich diese genehmigen lassen. Im Prüfungszeitraum wurden auch Anträge aus diesem <Grund abgelehnt

4. Datenschutzschulungen neuer Beschäftigte / regelmäßige Unterweisungen aller Beschäftigten / besondere Unterweisungen für Auszubildende

Alle 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 erst beantragt werden, wenn eine vollständige Einarbeitung erfolgt ist und die datenschutzkonforme Verarbeitung von personenbezogenen Daten auch im Homeoffice gewährleistet ist, d.h. mit dem Antrag müssen auch die im Homeoffice zu bearbeitenden Projekte genehmigt werden.

Während des Prüfungszeitraums wurden alle Beschäftigten aufgrund des erhöhten Sicherheitsrisikos regelmäßig sowohl im Umgang mit der erforderlichen Ausrüstung wie Antivirenprogramme 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 regelmäßig hingewiesen.

In Unternehmensweisungen festgeschrieben wurde ebenso 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. Auch der Download von diversen Hilfs-Apps, die nicht dem Datenschutzniveau entsprechen ist nicht gestattet.
Die Auszubildenden des Unternehmens erhielten im Rahmen der wöchentlichen betrieblichen Lehrveranstaltungen zusätzlich Datenschutzunterweisungen und Sicherheitshinweise zum datenschutzkonformen Verhalten im Unternehmen. Diese betrafen u.a. den Umgang mit personenbezogenen Kunden- und Interessentendaten, E-Mail-Anfragen und Kundentelefonaten. Die betreffenden datenschutzrechtlichen Inhalte wurden praxisnah erläutert und gemeinsam mit den Auszubildenden Sicherheitsmaßnahmen entwickelt.

5. Verpflichtung von Beschäftigten 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 Subunternehmen können der letzten Seite dieses Berichts entnommen werden und sind auch auf der Homepage unter Datenschutz / Subunternehmen veröffentlicht.

6. Unternehmensvorgaben zum Einsatz geprüfter Softwareanwendungen / Einsatz sicherer Kommunikationsmedien

a. **Verbindliche Unternehmensanweisungen:** Während des Prüfungszeitraums wurden die SEWOBE Unternehmensanweisungen aktualisiert und die Verwendung ausschließlich lizensierter Software, regelmäßige Updates der Sicherheitsprogramme sowie Sicherheitsvorkehrungen von PCs vorgeschrieben. Dies wurden in Zusammenarbeit der IT-Abteilung und der Datenschutzbeauftragten regelmäßig stichprobenartig kontrolliert. Die hierfür notwendigen technischen und organisatorischen Maßnahmen wurden in den ent-

sprechenden Verarbeitungstätigkeiten / Verfahrensbeschreibungen dokumentiert und im Datenschutzmanagementsystem bzw. im Handbuch abgelegt.

b. Reduzierung bzw. Vermeidung von E-Mail-Kundenverkehr: Der Empfang externer Kunden-E-Mails wurde bereits in den vergangenen Jahren in fast allen Abteilungen durch die 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 ggf. isoliert. HTML wird eliminiert und reiner Plain-Test (nicht formatiert) ausgegeben.

c. Sichere Kommunikationsmedien: Die SEWOBE bietet sichere Kundenschulungen über „TeamViewer“ oder „Teams“ mit Serverstandorten in Deutschland oder Europa an, damit personenbezogene Daten von Kommunikationsanbietern mit Serverstandorten in Drittländer, weder abfließen noch mitgeschnitten werden können. Teilweise wünschen Kunden ausdrücklich, dass Schulungen und Unterweisungen mittels unsicherer Kommunikationsanbieter (z. B. Zoom) aus Drittländern durchgeführt werden, die nicht das gleiche Datenschutzniveau aufweisen, wie es die EU-Datenschutzgrundverordnung vorschreibt. Die Beschäftigten der SEWOBE sind deshalb gehalten, die entsprechenden Kunden gemäß Vertrag zur Auftragsverarbeitung auf die Gefahren nicht datenschutzkonformer Daten-verarbeitungen hinzuweisen. Trotz der Hinweise bestehen einige Kunden weiterhin auf die Nutzung dieser kritischen Kommunikationsanbieter.

7. Gesicherte Neuentwicklungen von Softwarefunktionen / Evaluierung des Datenschutz-managementsystem (DSMS)

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 Online-Verwaltungssoftware. Die Entwicklung der Softwareprodukte wird von der Datenschutzbeauftragten fortlaufend, unter Betrachtung der Datenschutz- und Datensicherheitsanforderungen, begleitet, um die Einhaltung der hohen Qualitätsstandards der SEWOBE AG (u. a. Datensparsamkeit und Transparenz der Verarbeitung) von Beginn an zu gewährleisten.

8. Notfallmanagement: Notfallplan / Notfallhandbuch

Die SEWOBE hat für die nachfolgenden Szenarien einen Notfallplan aufgestellt, der den Teamverantwortlich zusätzlich in Printausfertigung bzw. auf Speichermedium ausgehändigt wird, um alle Beschäftigten im Notfall instruieren und einen geordneten Wiederanlauf, auch im Falle eines Serverausfalls gewährleiten zu können.

a. **Notfallplan**: Die SEWOBE AG hat im Prüfungsbericht den Notfallplan um Maßnahmen während der Pandemiezeit um den Quarantänefall ergänzt und evaluiert. Der Notfallplan umfasst folgende weitere Gefahrenfaktoren:
    - Cyberangriffe (Social Engineering=
    - Einbruch / Diebstahl / Vandalismus
    - Brand (Wasserschäden)
    - Elementarschäden (Naturkatastrophen) / Überschwemmungen
    - Ausfall von Führungspersonal - Vertretungsmanagement

    Im Fokus der Szenarien 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 turnusmäßig simuliert und der Wiederanlaufplan mit allen Beschäftigten trainiert.

    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 Systemausausfall Zugriff auf alle erforderlich 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.

9. 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 auch bereits in den Vorjahren, folgende weitere wichtige Kontroll-verfahren zur Gewährleistung des Datenschutzes und der Sicherheit der Verarbeitung bei der Technikgestaltung implementiert und fortgeführt, u. a.:

a. **Konzeptevaluierung:** 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 von 10 bis 17 Uhr die Systeme am Wochenende und an Feiertagen von Beschäftigten in Bereitschaftsdiensten beobachtet,

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 Abschluss dieser Zertifizierung ist für den Spätherbst 2023 geplant.

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 Audits.

Die nachfolgenden Siegel wurden im Zeitraum 2022 / 2023 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 - Erteilung oder Entzug von Zugriffsberechtigungen (z.B. Vorstandswechsel)

Während des Prüfungszeitzeitraums wurden von Organisationen (vertraglich Kunde oder Auftraggeber) mehrere Nachrichten per E-Mail oder Brief gesendet, die die SEWOBE aufforderten, Zugriffsrechte von bisher Berechtigten zu entziehen bzw. designierten Berechtigten zu zuteilen.
Die SEWOBE ist als Auftragnehmer und gemäß Vertrag zur Auftragsverarbeitung jedoch verpflichtet, ausschließlich auf Weisung von Berechtigten zu agieren. D. h. die Änderung von Berechtigungen, die nicht innerhalb der Organisationssoftware bzw. im Kundenportal hinterlegt wurden, können durch die SEWOBE weder autorisiert werden noch einen Zugriff erhalten. Dies obliegt einzig der Verantwortung und Weisung des berechtigten Auftraggebers 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 Zugriffsberechtigung vorliegt und der Antragsteller unter Vorlage eines Identitäts-nachweises 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 Kundenportal 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 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. Die Nutzung des Serviceportal ist im Softwarenutzungsvertrag verpflichtend geregelt.
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 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 Systemzugang SoftwareMANAGER: Newsletter-Versand bzw. E-Mail-Kommunikation

Nachdem das Double-Opt-in Verfahren und die 2-Faktor-Autentifizierung zu Beginn der Einführung nur zögerlich genutzt wurde, fand während des aktuellen Prüfzeitraums der automatisierte Einsatz dieser Option ohne Beanstandung 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. Auch der Systemzugang zur Verwaltungssoftware ist s

1.3 Sicherheitsaspekt Mitgliederportal

Das in der „Pro“ und Pro *Plus* Version erhältliche *Mitglieder- bzw. Kundenportal* gewährleistet eine sichere Kommunikation innerhalb der Kunden-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 Geschäfts-räumen. 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 Zugriffs-berechtigung, 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 Datenverarbeitungs-vorlagen
- 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 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 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

Augsburg, den 28.05.2023

Geprüft:

Datenschutz Serviceteam

DSGVO-KONFORM Qualifizierter Datenschutz Datenschutz - Serviceteam

Datenschutzbeauftragte:

Dipl.-Ing. Heike Lenz

Augsburg den 30.05.2023

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 05/2023

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

	Firma	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** (Business Unit mit acmeo) Backup & Recovery www.acmeo.eu https://infinigate.de/Technologien/	Richard-Reitzner-Allee 8 85540 Haar / München

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.

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.