Prüfbericht 2019

zu den technischen und organisatorischen Maßnahmen gem. 32 DSGVO i.V. m. § 9 des Vertrages zur Auftragsverarbeitung zwischen SEWOBE und Auftraggeber zur Gewährleistung der Sicherheit der Verarbeitung

Unternehmen	SEWOBE GmbH, Werner Haas Str. 8, 86153 Augsburg vertreten durch die Geschäftsführer Eiko Trausch und Thomas Weishaupt
Ort	Unternehmenssitz: Werner-Haas-Str. 8, 86153 Augsburg
Prüfer	Datenschutzkoordination Heike Lenz (Dipl.-Ing.) in Zusammenarbeit mit dem Institut für Datenschutz in Augsburg
Prüfzeitraum	2018 / 2019
Datum	22.03.2019

Gegenstand und Inhalt des Prüfberichts

Der Prüfbericht 2019 dokumentiert im Folgenden die technischen und organisatorischen Maßnahmen der SEWOBE zur Sicherheit der Verarbeitung personenbezogener Daten gem. Art. 32 DSGVO im Rahmen der Auftragsverarbeitung.

I. Organisatorische Maßnahmen

1. **Dokumentation der Datenschutz- und IT-relevanten Maßnahmen**
   Die SEWOBE führt ein umfassendes digitales **Datenschutzmanagementsystem** (DSMS) und dokumentiert alle relevanten Verarbeitungstätigkeiten in einem Verzeichnis (VVT) im DSMS.
   Zur konsequenten Fehlervermeidung sind für alle wichtigen Verarbeitungstätigkeiten Checklisten vorhanden, die konsequent abzuarbeiten sind.

2. **Betrieblicher Datenschutzbeauftragter / Datenschutzkoordination**
   Die SEWOBE verfolgt umfassende Datenschutzmaßnahmen, die durch einen externen Datenschutzbeauftragten und eine interne Datenschutzkoordination betreut und regelmäßig überprüft werden. Kontaktdaten: datenschutz@sewobe.de

3. **Mitarbeiterschulungen zu Datenschutz und IT-Sicherheit**
   Alle Mitarbeiter der SEWOBE werden mindestens zweimal im Jahr in Workshops geschult und regelmäßig zusätzlich in ihren individuellen Arbeitsbereichen unterwiesen.

Alle sicherheitsrelevanten Verhaltensweisen bei der Verarbeitung personenbezogener Daten werden in Unternehmensanweisungen festgeschrieben.

4. **Verpflichtung auf Vertraulichkeit (Datengeheimnis)**
   Alle Mitarbeiter und externen Dienstleister der SEWOBE werden auf Vertraulichkeit verpflichtet, ebenso auf das Fernmeldegeheimnis und auf die Wahrung von Geschäftsgeheimnissen, jeweils mit Wirkung über das Ende der Tätigkeit hinaus.

5. **Gütesiegel bzw. Zertifizierungen der SEWOBE Software Services** (MANAGER)
   - **„Trusted Cloud e.V."** zertifizierter Service / Bundesministerium für Wirtschaft und Energie in Zusammenarbeit mit Kompetenznetzwerk Trusted Cloud e. V.: Im Vordergrund der Aktivitäten steht die Schaffung von Transparenz und Vertrauen in Cloud-Technologien: Transfer von anwenderorientiert aufbereitetem Wissen rund um Cloud Computing und Listung von geprüften Cloud-Anwendungen.
     Das Kompetenznetzwerk Trusted Cloud e.V. fördert den effizienten, sicheren und rechtskonformen Einsatz von Cloud-Technologien: https://www.trusted-cloud.de/de/projekt . Weitere Informationen finden Sie auch 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"** / 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

6. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
   - Regelmäßige Aktualisierung und Fortschreibung des Datenschutz und IT-Sicherheitskonzeptes der SEWOBE.
   - Einsatz von verfahrensunabhängigen Plausibilitäts- und Sicherheitsprüfungen (u.a. interne Erstellung von Prüfberichten zur Sicherheit der eingesetzten Server).

II. Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

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

1.1. Zutrittskontrolle

Folgende Maßnahmen werden in den Räumen der SEWOBE getroffen, um Unbefugten den räumlichen Zutritt zu solchen Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogener Daten verarbeitet oder genutzt werden:

- Die Server befinden sich im Serverraum des Auftragnehmers bzw. in einem zertifizierten deutschen Rechenzentrum. Zugang zum Server ist nur autorisiertem Personal gestattet, elektronisch gesichert und nachprüfbar.
- Besucher bzw. Dritte haben Zutritt nach Anmeldung zu Räumlichkeiten der SEWOBE (Empfang mit Anmeldung / Regelung für Firmenfremde)
- Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde)
- Türsicherung / Schlüsselregelung (Einsatz elektronischer Zutrittsmedien)
- Anwesenheitsaufzeichnung anhand von Zugangsprotokollen
- Einsatz elektronischer Sicherheitsschlösser in alle Räume mit sensibler Infrastruktur.
- Sorgfältige Auswahl und Verpflichtung auf Vertraulichkeit und Geheimhaltung des Reinigungspersonals

1.2. 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 Datenverarbeitungssystemen für zu Unbefugte zu verhindern und umfassen folgende Maßnahmen:

- Authentifikation 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
- Rechtezuweisungen sind an Zugangskennungen gebunden (Einteilung nach Administrator, Benutzer etc.)
- Zuordnung einzelner Terminals
- Bildschirmsperre bei Abwesenheit mit jeweiliger Passwort-Aktivierung
- Einsatz von VPN Technologien
- Prüf-, Abstimm- und Kontrollsysteme

1.3. Zugriffskontrolle

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

- Die SEWOBE Software beinhaltet ein Berechtigungskonzept und ermöglicht durch eine Historie die Erstellung von Benutzerprofilen / Regelung der Zugriffsberechtigung

- Verwaltung der Rechte durch System-Administrator
- Beschränkung der Administratorrechte auf das Notwendigste / Überwachung durch technischer Geschäftsleiter
- Arbeitsanweisungen und Bearbeitungsverfahren für Datenerfassungsvorlagen
- Firewall und Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches sind im Einsatz.
- Gesicherte Nutzung von USB Schnittstellen
- Verschlüsselung von (mobilen) Datenträgern
- Protokollierung von Zugriffen auf Anwendungen
- Kontrollierte physische Vernichtung von Datenträgern durch zertifizierte Unternehmen (Documentus Bayern / Reisswolf)
- Sichere Aufbewahrung von Datenträgern
- Regelmäßige Überprüfung der Clear Desk Policy
- Firewall und Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches sind im Einsatz.
- Verschlüsselung „unterwegs" (VPN)
- Eng begrenzte Zugriffsberechtigung auf Datenbestände und Funktionen
- Vermeidung von E-Mail-Verkehr durch den Einsatz eines Serviceportals für die Kundenkommunikation.

1.4. 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 Back-ups etc.
- Tabellarische Mandantentrennung sowie Trennung von Daten verschiedener Auftraggeber / Mandanten
- Datenbankrechte - Zuordnung durch technische Geschäftsleitung
- Trennung von Test- und Live-Umgebungen

1.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in der Weise, dass der Personenbezug von Daten nicht vollständig hergestellt werden kann, z.B. durch Zuweisung von Kundennummern / Mitgliedernummern.

1.6. 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 Verschlüsselung
- Kommunikation über SEWOBE Serviceportal über ein Ticketsystem zur Vermeidung von Kommunikation bzw. von Datenübertragungen via E-Mail); Bewerbungsportal.

2. Integrität (Art. 32 Abs. 1 lit b. DSGVO) / Authentizität

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

2.1. Weitergabekontrolle

Maßnahmen zur Vermeidung von unbefugtem Lesen, Kopieren, Veränderung oder Verlust während des Transports oder der Speicherung und 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 von Übermittlung / Identitätsprüfung der Empfänger
- Dokumentation und stete Aktualisierung der Hard- und Software über eine Inventarübersicht.
- E-Mail Verschlüsselung via ZIP Datei – Abwicklung vorzugsweise über Versand Nutzung des SEWOBE Serviceportals.
- Entsorgung von Festplatten, Disketten und Akten durch zertifizierte Unternehmen und entsprechende Nachweise.

2.2. Eingabekontrolle / Verarbeitungskontrolle

Maßnahmen zur Gewährleistung der Überprüfung und Feststellung welcher Benutzer den Datenbestand eingegeben, verändert oder gelöscht hat:

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

2.3. Dokumentationskontrolle

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

- Führung eines Verarbeitungsverzeichnisses (VVZ) innerhalb des Datenschutzmanagementsystems Protokollierung (DSMS)
- Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration.
- Zulässigkeiten von Datentransfers sind in den jeweiligen Verarbeitungstätigkeiten dokumentiert.

2.4. Auftragskontrolle

Gewährleistung der Verarbeitung von personenbezogenen Daten durch den Auftragnehmer ausschließlich auf Weisung des Auftraggebers:

- Jegliche Aktivität basiert auf einem Vertrag zur Auftragsverarbeitung bzw. auf Basis eines Auftrages.
- Mündliche Aufträge sind umgehend schriftlich zu bestätigen.
- Vor Auftragsübernahme erfolgt die Prüfung der Berechtigung des Auftraggebers; berechtigte Personen sind im Vertrag bzw. in der SEWOBE Software hinterlegt.
- Formalisierung der Auftragserteilung innerhalb des SEWOBE Ticketsystems, Auftragsausführung erst nach Freigabe durch den berechtigten Auftraggeber
- Regelungen zur Fernwartung via TeamViewer
- Verpflichtende Datenschutzmaßnahmen beider Parteien in mindestens gleichem Umfang

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

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

- Unterbrechungsfrei Stromversorgung (USV Anlage) / Überspannungsschutz
- Online-Überwachung von Temperatur und Feuchtigkeitsmessung im Serverraum
- Klimaanlage im Serverraum
- Feuer- und Rauchmelder
- Schutzsteckdosen im Serverraum
- Feuerlöschgeräte an mehreren Stellen in den Räumen der Räumen der SEWOBE
- Regelmäßige Backup-Lösungen an unterschiedlichen Standorten
- Virenschutz
- Regelmäßige Evaluierung und Aktualisierung des Notfallkonzepts

3.2. Belastbarkeit (Widerstandsfähigkeit von Systemen und Dienstleistungen)

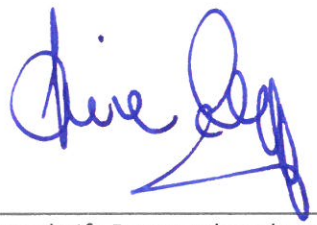
Maßnahmen zur Gewährleistung der Aufrechterhaltung von technischen Systemen bei Störung bzw. Teilausfällen:

- 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

---

Ende der technischen und organisatorischen Maßnahmen

Geprüft:	
Augsburg, den 4.04.2019	Augsburg, den 04.04.2019
	
Unterschrift Datenschutzkoordination	Unterschrift externer Datenschutzbeauftragter

Liste der beauftragten Subunternehmer (Stand 03/2019)

1. Die SEWOBE GmbH erklärt, dass die nachfolgenden Subauftragnehmer zur Unterstützung eingesetzt werden.

	Firma	Adresse
1	1&1 IONOS Cloud GmbH (vormals ProfitBricks GmbH)	Eigendorfer Straße 57 56410 Montabaur
2	TelemaxX Telekommunikation GmbH	Amalienbadstraße 41 Bau 61 76227 Karlsruhe Deutschland
3	acmeo GmbH (MSP Backup & Recovery)	Mailänder Str. 2 30539 Hannover

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.