Prüfbericht 2020

zu den technischen und organisatorischen Maßnahmen gem. 32 DSGVO i.V. m. § 9 des Vertrages zur Auftragsverarbeitung zwischen der SEWOBE AG als Auftragnehmerin und dem Auftraggeber zum Nachweis der Sicherheit bei der Verarbeitung personenbezogener Daten

Unternehmen:	SEWOBE AG, Werner Haas Str. 8, 86153 Augsburg vertreten durch die Vorstände Eiko Trausch und Thomas Weishaupt
Prüfort:	Unternehmenssitz: Werner-Haas-Str. 8, 86153 Augsburg
Prüfer:	Datenschutz Serviceteam Augsburg, Koordination Dipl.-Ing. Heike Lenz
Prüfzeitraum:	2019 / 2020
Datum:	28.05.2020

Inhalt

Prüfberichtsgegenstand

Gemäß § 9 des Vertrages zur Auftragsverarbeitung verpflichtet sich die Auftragnehmerin, SEWOBE AG, einen Jahresprüfbericht zu erstellen, um den Auftraggeber bei seiner Kontrollpflicht zu unterstützen.
Der Prüfbericht 2019/2020 dokumentiert in den Kapiteln I. und II. die organisatorischen und technischen Maßnahmen der SEWOBE AG und dient als Nachweis der Einhaltung des Datenschutzes und der Sicherheit bei der Verarbeitung personenbezogener Daten gem. Art. 32 DSGVO im Rahmen der Auftragsverarbeitung.
In Kapitel III. werden die Datenschutzmaßnahmen erläutert, die aufgrund der COVID-19 Pandemie unternommen wurden, um die Sicherheit der Verarbeitung auch in Ausnahmezeiten zu gewährleisten.

I. Allgemeine organisatorische Maßnahmen zum Datenschutz

1. **Dokumentation der Datenschutz- und IT-relevanten Maßnahmen**
   Die SEWOBE AG führt ein umfassendes digitales **Datenschutzmanagementsystem** (DSMS) und dokumentiert alle relevanten Verarbeitungstätigkeiten im Verzeichnis der Verarbeitungstätigkeiten (VVT). Eine Evaluierung der Prozesse erfolgt regelmäßigen Abständen durch die Verantwortlichen mit ihrer Datenschutzbeauftragten.
   Zur Fehlervermeidung sind für alle wichtigen Verarbeitungstätigkeiten personenbezogener Daten Checklisten vorhanden, die von allen Beschäftigten nachweislich abzuarbeiten und vorzulegen sind, d.h. dass ein Vorgang erst nach Dokumentation aller Vorgaben abgeschlossen werden darf.

2. **Externe Datenschutzbeauftragte**
   Die SEWOBE AG ergreift umfangreiche Maßnahmen zum Datenschutz, die regelmäßig durch eine externe Datenschutzbeauftragte betreut und evaluiert werden.
   Kontaktdaten: datenschutz@sewobe.de.

3. **Datenschutzschulungen der Beschäftigten**
   Die Beschäftigten der SEWOBE AG werden mehrmals im Jahr in umfassenden Datenschutz-Workshops geschult und in regelmäßigen Abständen in ihren individuellen Arbeitsbereichen unterwiesen und geprüft.
   Alle sicherheitsrelevanten Vorgaben für die datenschutzkonforme Verarbeitung personenbezogener Daten werden in Unternehmensanweisungen festgeschrieben und die Beschäftigten in Schulungen ausführlich über Inhalte und Auswirkungen informiert.

4. **Verpflichtung auf Vertraulichkeit (Datengeheimnis)**
   Beschäftigte und externe Dienstleister der SEWOBE AG werden auf Vertraulichkeit, das Fernmeldegeheimnis und auf die Wahrung von Geschäftsgeheimnissen verpflichtet und über arbeits- und strafrechtliche Konsequenzen belehrt, die jeweils mit Wirkung über das Ende der Tätigkeit hinaus gelten.

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

   - Die SEWOBE AG hat sich mit ihren Services vom „Trusted Cloud e.V." erfolgreich überprüfen lassen. Hierbei handelt es sich um einem 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 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/.
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

6. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** (Art. 32 Abs. 1 lit. d) DSGVO und Art. 25 Abs. 1 DSGVO)
   Die SEWOBE AG hat u. a. folgende wichtige Kontrollverfahren zur Gewährleistung des Datenschutzes und der Sicherheit der Verarbeitung bei der Technikgestaltung implementiert, 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).

II. Technische und organisatorische Maßnahmen

1. Sicherheitsmaßnahmen innerhalb der SEWOBE Software MANAGER-Lösungen

Um die Sicherheit der Nutzer*innen zu erhöhen, hat die SEWOBE AG nachfolgende Verfahren im Unternehmen und innerhalb der Software implementiert:

1.1 Serviceportal / Verzicht auf E-Mail-Kommunikation

Die SEWOBE AG hat ihre E-Mail-Kommunikation aus Sicherheitsgründen eingestellt und hält für ihre Nutzer*innen das SEWOBE Serviceportal bereit, über das die gesamte Kommunikation im geschützten Bereich erfolgt.
Das Serviceportal verfügt über einen passwortgesicherten Log-in und bietet u. a. folgende Services für ihre Nutzer*innen an: Ticketportal für Support-Anfragen, Dokumente zur Hinterlegung von Verträgen, Finanzstatus (Hinterlegung von Rechnungen etc.), Ideenportal u.v.m.

Der Auftraggeber bzw. die bevollmächtigten Nutzer*innen werden vertraglich dazu verpflichtet, das Serviceportal für (Support-)Anfragen zu nutzen und aufgefordert, keine sensiblen Daten per E-Mail zu senden.

1.2 Double Opt-in Verfahren - Newsletter Versand bzw. E-Mail- Kommunikation

In den Software MANAGER-Versionen „Basic" und „Pro" wird das Double Opt-in Verfahren automatisiert bereitgestellt. Die SEWOBE AG empfiehlt dringend den Einsatz dieser Option, da nur so sichergestellt werden kann, dass die angegebenen E-Mail-Adressen in den Newsletter-Anträgen auch identisch sind mit den tatsächlichen Inhaber*innen der E-Mail Adressen.

1.3 Mitgliederportal für den Auftraggeber

Das in der „Pro" Version erhältliche Mitglieder- bzw. Kundenportal gewährleistet eine sichere Kommunikation innerhalb der Organisation bzw. des Unternehmens. Im Mitgliederportal können sämtliche Informationen für Mitglieder bzw. Bevollmächtigte im gesicherten Bereich zum Downloade hinterlegt werden, ohne dass diese per E-Mail versendet werden müssen.

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

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, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

- Türsicherung mit elektronischer Zutrittsregelung, die zusätzlich kameraüberwacht ist.
- Beschäftigte der SEWOBE AG erhalten über ein elektronisches Schließsystem Zutritt zu den allgemeinen Geschäftsräumen. Deren Daten werden protokolliert und in regelmäßigen Abständen wieder gelöscht.
- Einsatz zusätzlicher elektronischer Sicherheitsschlösser in allen Räumen mit sensibler Infrastruktur, z.B. erhält nur ein festgelegter Personenkreis Zugang zum Serverraum. Der Zutritt wird ebenfalls protokolliert.
- Besucher*innen bzw. Dritte haben nur Zutritt zu den Geschäftsräumen der SEWOBE AG nach vorheriger Anmeldung beim Empfang und können sich innerhalb der Geschäftsräume nicht frei bewegen.
- Es liegen schriftliche Festlegungen 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 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, 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 Back-ups 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:

- TSL / SSL Verschlüsselung
- 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 (Art. 32 Abs. 1 lit. b) DSGVO) / 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 eine Inventarübersicht (Entwicklung eines InventarMANAGERs).
- Im Ausnahmefall: E-Mail-Verschlüsselung via ZIP Datei – üblich ist jedoch die Abwicklung über das SEWOBE Serviceportal.
- 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, welcher Benutzer bzw. Beschäftigte den Datenbestand eingegeben, verändert oder gelöscht hat:

- Vergabe von Zugangsregelungen und Benutzungsberechtigungen zur SEWOBE Software
- 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 Verarbeitungsverzeichnisses (VVZ) innerhalb des Datenschutzmanagementsystems (DSMS), d.h. Dokumentation aller relevanten Verarbeitungstätigkeiten.
- Zulässigkeiten von Datentransfers sind in den jeweiligen Verarbeitungstätigkeiten dokumentiert.

- 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
- Verpflichtende Datenschutzmaßnahmen beider Parteien in mindestens gleichem Umfang

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

4.1. Verfügbarkeitskontrolle

Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten und IT-Systemen 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

III. Aktuelles (Stand 25.05.2020)

1. Bericht über Maßnahmen aufgrund der COVID-19 Pandemie

Aktualisierung des Notfallplans / Ergänzung um Pandemie- bzw. Quarantänemaßnahmen
Nach Bekanntwerden der Corona Fälle im europäischen Raum hat die SEWOBE AG Anfang März 2020 gemeinsam mit ihrer Datenschutzbeauftragten den bestehenden Notfallplan aktualisiert und um die Maßnahmen im Falle einer Pandemie / Quarantäne ergänzt.
Über die Inhalte des Notfallplans wurden die Beschäftigten umgehend informiert und erhielten Kontaktdaten und weitere Informationen für das Verhalten in einem Notfall sowie Anweisungen zum Wiederanlaufplan.
Zudem wurde zusätzliche Hard- und Software angeschafft, um die Beschäftigten für einen Notfall und eine Tätigkeit im Home-Office datenschutzkonform entsprechend ausstatten zu können und eine gesicherte Kommunikation auch außerhalb des Geschäftssitzes zu gewährleisten.
Jeder interne und mobile PC wurde, sofern noch nicht geschehen, mit einer VPN Verbindung ausgestattet. Für die Teamarbeit wurde ein Kommunikationstool ausgewählt, dessen Server in Europa verortet sind. Somit wird gewährleistet, dass die Unternehmenskommunikation aufgrund der erweiterten Infrastrukturmaßnahmen unverändert sicher fortgeführt werden kann.

Schulung der Beschäftigten der SEWOBE AG am 13.03.2020
Verhalten im Notfall / Home-Office Regularien
Alle Beschäftigten der SEWOBE AG erhielten bereits am 13.03.2020 eine umfassende Schulung, wie das Unternehmen im Falle einer Pandemie bzw. einer Quarantäne seine Geschäftstätigkeit fortsetzen kann, ohne das bisherige Schutzniveau für Kunden- und Beschäftigtendaten zu unterschreiten.
Hierzu wurde das Verhalten im Notfall ausführlich geschult und in einer Unternehmensanweisung dokumentiert. Zudem wurden die Home-Office Regularien angepasst und auf alle Beschäftigten ausgeweitet, in dem die unterschiedlichsten häuslichen Situationen Berücksichtigung gefunden haben.

Evaluierung der Home-Office Regularien und des Hygienekonzepts am Geschäftssitz
Die Auswirkungen der COVID-19 Pandemie auf die sichere Geschäftsführung werden von den verantwortlichen Vorständen der SEWOBE AG und der Datenschutzbeauftragten wöchentlich bewertet und für die Beschäftigten im Home-Office ggf. neu justiert. Für die Beschäftigten am Geschäftssitz wird das Raumnutzungs- und Hygienekonzept regelmäßig überarbeitet und auch für Besucher Verhaltensregeln aufgestellt, die über die Homepage bzw. am Geschäftssitz bekannt gemacht werden.
Für alle Beschäftigten und Besucher wurde frühzeitig eine ausreichende Anzahl von Masken und Desinfektionsmitteln geordert und bereitgehalten.

2. Neuer Kundenservice:

Muster-Verfahrensdokumentation zur Beitragsrechnung und Belegablage

Die SEWOBE AG setzt für ihre Verwaltung die Verwaltungssoftware ein, die auch die Auftraggeber (Kunden) verwenden.
Um die Auftraggeber (Kunden) bei der Verfahrensdokumentation für die Beitrags-abrechnung und Belegablage zu unterstützen, die von der GoBD* vorgeschriebenen wird, stellt die SEWOBE AG ab sofort ein Muster zu Verfahrensdokumentation zum Download in der Online-Hilfe bereit.

---

*Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff

Geprüft:	Augsburg, den 28.05.2020
Datenschutzbeauftragte: Datenschutz Serviceteam	Dipl.-Ing. Heike Lenz
Verantwortliche Vorstände SEWOBE AG	Augsburg den 28.05.2020
Thomas Weishaupt, techn. Vorstand	Eiko Trausch, Kaufm. Vorstand

Anlage 1

Liste der beauftragten Subunternehmer (Stand 03/2019)

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

	Firma	Adresse
1	1&1 IONOS Cloud GmbH (Datenspeicherung)	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.