Vertrag zur Auftragsverarbeitung

Zwischen
(Organisationsname)

Microsoft Business User Forum e.V. (mbuf)

geschäftsansässig:
(Adresse der Organisation)

Werner-von-Siemens-Str. 2
64319 Pfungstadt

Vertreten durch:
(Name der Vertretungsberechtigten)

Ralph Alkemade, Sprecher des Vorstandes
Stefan Busch, Schatzmeister

- im Folgenden „Auftraggeber"

und

SEWOBE GmbH
Werner Haas Str. 8
86153 Augsburg
vertreten durch die beiden Geschäftsführer
Eiko Trausch und Thomas Weishaupt

- im Folgenden „Auftragnehmer" -

PRÄAMBEL

Der Vertrag zur Auftragsverarbeitung (AV Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien gemäß. Art. 28 Abs. 3 der Datenschutzgrund-verordnung (DSGVO), die sich aus der Erbringung der Leistungen des zwischen den Parteien bereits bestehenden Softwaremietvertrages ergeben und findet Anwendung auf alle Tätigkeiten, die mit dem Softwaremietvertrag in Verbindung stehen und bei denen Beschäftigte des Auftragnehmers oder dessen Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.
Dieser Vertrag zur Auftragsverarbeitung ersetzt zudem die bisherige Vereinbarung zur Auftragsdatenverarbeitung (ADV), sofern eine vereinbart wurde.

§ 1 Gegenstand, Dauer und Spezifizierung des Vertrags zur Auftragsverarbeitung

(1) Dieser Vertrag umfasst die Verarbeitung von personenbezogenen Daten des Auftraggebers durch den Auftragnehmer gemäß Softwaremietvertrag (Hauptleistungsvertrag).

(2) Zweck, Umfang und Art der verarbeiteten Daten ergeben sich aus den Anforderungen des Auftraggebers in Verbindung mit dessen Einsatz der Software-Lösung innerhalb seiner Organisation.

(3) Die Laufzeit des Vertrages zur Auftragsverarbeitung richtet sich nach der Laufzeit des Softwaremietvertrages, sofern sich aus den Bestimmungen dieses Vertrages nicht darüberhinausgehende Verpflichtungen ergeben.

(4) Dieser Vertrag wird gültig mit dem Hochladen der gegengezeichneten Fassung im Serviceportal des Auftragnehmers.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer (Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO) verarbeitet nur personenbezogene Daten, die zur Erfüllung seiner Vertragstätigkeit erforderlich sind und solche Daten, die der Auftraggeber während des Vertragsverhältnisses anweist. Art und Umfang der Tätigkeiten sind im Softwaremietvertrag bzw. in der Leistungsbeschreibung konkretisiert.

(2) Die Weisungen des Auftraggebers ergeben sich aus dem Softwaremietvertrag. Mündliche Weisungen des Auftraggebers sind unverzüglich in schriftlicher oder Textform durch das Anlegen eines Tickets im Serviceportal zu bestätigen. Vom Vertrag abweichende Weisungen werden als Antrag auf Leistungsänderung behandelt.

(3) Die Speicherung und Verarbeitung der Daten findet ausschließlich in Rechenzentren auf dem Gebiet der Bundesrepublik Deutschland statt.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisung des Auftraggebers verarbeiten, es sei denn, dass er nach geltendem Recht zur Verarbeitung verpflichtet ist.
Er beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung und informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstoßen könnte. Der Auftragnehmer darf die Weisung so lange aussetzen, bis diese vom Auftraggeber bestätigt oder abgewendet wurde.

(2) Der Auftragnehmer gewährleistet, dass es den Mitarbeitern, die mit der Verarbeitung der Daten des Auftraggebers beauftragt sind, untersagt ist, Daten außerhalb der Weisungen zu verarbeiten. Ferner verpflichtet der Auftragnehmer alle Mitarbeiter zur Vertraulichkeit, die mit der Verarbeitung personenbezogener Daten beauftragt sind. Das Datengeheimnis und die Verschwiegenheitspflicht bestehen auch nach Beendigung der Tätigkeit fort.

(3) Der Auftragnehmer wird die innerbetriebliche Organisation seines Unternehmens so gestalten, dass diese den Anforderungen des Datenschutzes gerecht werden. Er verpflichtet sich, technische und organisatorische Maßnahmen gem. Art. 32 DSGVO zu treffen, die dem angemessenen Schutz der Daten des Auftraggebers und den Gesetzesanforderungen entsprechen, um die Daten des Auftraggebers vor Missbrauch und Verlust zu schützen. Die technischen und organisatorischen Maßnahmen gem. Anlage 1 stellen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicher.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen und eine Änderung der getroffenen Sicherheitsmaßnahmen vorzunehmen, wobei jedoch sichergestellt sein muss, dass

das vorherige Schutzniveau nicht unterschritten wird.

(5) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Die Vergütung des Auftragnehmers erfolgt nach Aufwand auf Basis der zum Zeitpunkt der Leistungserbringung gültigen Honorarsätzen.

(6) Dem Auftragnehmer sind die Informationspflichten bezgl. der Verletzungen des Schutzes personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen bekannt. Er ist verpflichtet, Datenschutzverletzungen zu dokumentieren und den Auftraggeber unverzüglich zu informieren. Auch ist die zuständige Aufsichtsbehörde bei Verletzung datenschutzrechtlicher Bestimmungen spätestens 72 Stunden nach Kenntnis zu benachrichtigen, ebenso die hiervon Betroffenen.

(7) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt und dessen Kontaktdaten unter https://www.sewobe.de/datenschutz/datenschutzbeauftragter/ veröffentlicht. Konsultiert der Auftraggeber den Datenschutzbeauftragten des Auftragnehmers, so trägt der Auftraggeber die hierfür anfallenden Kosten gemäß geltenden Honorarsätzen des Datenschutzbeauftragten.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber („Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO) ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Zulässigkeit der Datenverarbeitung gemäß Art. 6 DSGVO allein verantwortlich, ebenso für die Wahrung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO (Recht / Haftung auf Schadenersatz), verpflichtet sich der Auftragnehmer, den bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Die Vergütung des Auftragnehmers erfolgt nach Aufwand auf Basis der zum Zeitpunkt der Leistungserbringung gültigen Honorarsätzen.

(3) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten datenschutzrechtlicher Bestimmungen feststellt oder ihm Verletzungen des Schutzes personenbezogener Daten bekannt werden. Er ist verpflichtet, alle Verletzungen des Schutzes personenbezogener Daten umfassend zu dokumentieren. Datenschutzrechtliche Verletzungen sind vom Auftraggeber spätestens 72 Stunden ab Kenntnisnahme der zuständigen Aufsichtsbehörde zu melden bzw. ggf. die Betroffenen zu informieren.

(4) Der Auftraggeber legt die Maßnahmen zur Rückgabe der Datenträger und / oder Löschung der gespeicherten Daten nach Beendigung oder durch Weisung fest, sofern diese im Hauptleistungsvertrag nicht bereits geregelt sind. Entstehende Kosten durch die Herausgabe oder Löschung von Daten (z.B. Migration an einen Dritten), trägt der Auftraggeber.

(5) Der Auftraggeber nennt dem Auftragnehmer den zuständigen Ansprechpartner für Datenschutzbelange, die sich im Rahmen des Vertrags ergeben können.

(6) Der Auftraggeber erstattet dem Auftragnehmer alle Aufwendungen für Kontrollmaßnahmen, die über den jährlichen Prüfbericht gemäß § 9 Abs.2 und 3 dieses Vertrages hinausgehen, insbesondere für Unterstützungsleistungen des Auftragnehmers oder der von ihm Beauftragten, die im Rahmen weiterer etwaiger gesetzlicher Verpflichtungen entstehen können.

§ 5 Durchsetzung der Rechte betroffener Personen

(1) Wendet sich eine betroffene Person mit dem Recht zur Auskunft, Berichtigung, Löschung, Sperrung oder Übertragbarkeit an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung des Auftraggebers nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter.

(2) Soweit vereinbart, unterstützt der Auftragnehmer den Auftraggeber auf dessen Weisung im Rahmen seiner Möglichkeit bei der Durchsetzung der in Artikeln 32 bis 36 DSGVO genannten Pflichten. Unterstützungsleistungen vergütet der Auftraggeber in Höhe der jeweils geltenden Honorarsätze. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Löschung von Daten und Rückgabe von Datenträgern, Insolvenzregelung

(1) Der Auftragnehmer berichtigt, löscht und sperrt die vertragsgegenständlichen Daten nur nach Weisung des Auftraggebers. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung durch den Auftraggeber nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits entsprechendes vereinbart wurde. Die Vergütung berechnet sich nach den jeweils geltenden Honorarsätzen.

(2) Nach Beendigung des Softwaremietvertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände dem Auftraggeber auf dessen Anforderung und Kosten auszuhändigen oder nach Weisung datenschutzgerecht zu vernichten, sofern nicht anderslautende Gesetze diesem Interesse entgegenstehen. Gleiches gilt für Test- und Ausschussmaterial.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen, auch über das Vertragsende hinaus, aufzubewahren.

(4) Der Auftraggeber ist Alleinberechtigter an seinen Daten. Sollten die Daten des Auftraggebers beim Auftragnehmer durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Es gelten zudem die weiteren Bedingungen des Softwaremietvertrages. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten i.S.d. Datenschutz-Grundverordnung (DSGVO) grundsätzlich beim Auftraggeber liegen.

§ 7 Unterauftragsverhältnisse / Subunternehmen

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Leistungen aus dem Softwaremietvertrag beziehen.
Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

(2) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Wahrung seiner vertraglich vereinbarten Pflichten Subunternehmen zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers, angemessene und gesetzeskonforme vertragliche Vereinbarungen nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) In der **Anlage 2** zu diesem Vertrag sind die vom Auftragnehmer zu diesem Zeitpunkt eingesetzten und bereits geprüften Subunternehmer für die Erfüllung der wesentlichen Vertragspflichten aufgeführt (z.B. Rechenzentren etc.)

(4) Änderungen oder Ergänzungen der beauftragten Subunternehmen veröffentlicht der Auftragnehmer auf der Website des Auftragnehmers unter dem Link: https://www.sewobe.de/datenschutz/subunternehmer

(5) Der Auftraggeber kann der Änderung oder Ergänzung aus wichtigem datenschutzrechtlichem Grund innerhalb einer Frist von vier Wochen nach Bekanntmachung gegenüber dem Auftragnehmer widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösung zwischen den Parteien nicht möglich, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(6) Beauftragt ein Subunternehmer des Auftragnehmers seinerseits einen Subunternehmer, bedarf es der Genehmigung des Auftraggebers, zumindest aber einer Information (Systemnachricht / E-Mail) innerhalb einer angemessenen Frist von vier Wochen über die Erfüllung der Vorgaben nach § 7 Absatz 2 dieses Vertrages.

(7) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten.

§ 8 Haftung

(1) Der Auftragnehmer haftet, gleich aus welchem Rechtsgrund, auf Schadenersatz oder Ersatz vergeblicher Aufwendungen in voller Höhe nur für Schäden des Auftragsgebers durch vorsätzliches oder grob fahrlässiges Verhalten, im Fall der Übernahme ausdrücklicher Garantien sowie zugesicherten Eigenschaften, bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, für Ansprüche aus Produkthaftung sowie im Fall zwingender gesetzlicher Regelungen.

(2) Bei der Verletzung wesentlicher Vertragspflichten (Kardinalpflichten) haftet der

Auftragnehmer - unbenommen des vorstehenden Absatzes - begrenzt auf den vertragstypischen, bei Vertragsschluss vernünftigerweise vorhersehbaren Schaden. Bei Kardinalpflichten handelt es sich um Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglichen und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf. Als vertragstypischer, vorhersehbarer Schaden gilt ein Schaden in Höhe der Jahresmiete des Kunden.

(3) Soweit die Haftung des Auftragnehmers gegenüber dem Kunden beschränkt oder ausgeschlossen ist, gilt dies entsprechend für gesetzliche Vertreter, Arbeitnehmer, freie Mitarbeiter und sonstige Erfüllungs- bzw. Verrichtungsgehilfen. Über Ansprüche von Dritten, die über die vorstehenden Regularien hinausgehen, stellt der Auftraggeber den Auftragnehmer frei.

(4) Gesetzlich zwingende Haftungsregelungen bleiben hiervon unberührt.

§ 9 Nachweismöglichkeiten der Datensicherheit

(1) Dem Auftraggeber sind die zu erbringenden technischen und organisatorischen Maßnahmen bekannt, die in Anlage 1 spezifiziert sind. Ihm ist bekannt, dass er die Verantwortung dafür trägt, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(2) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten zu den technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO mit geeigneten Mitteln nach, damit der Auftraggeber sein Kontrollrecht wahrnehmen kann. Der Auftragnehmer wird deshalb mit den Datenschutzbeauftragten einen jährlichen Prüfbericht erstellen, in dem die Einhaltung der vereinbarten Schutzmaßnahmen und deren Wirksamkeit aufgeschlüsselt sind.

(3) Der Prüfbericht kann auch durch eine anerkannte Zertifizierung gemäß Art. 42 DSGVO ersetzt werden. Die Einhaltung der Aktualität der Zertifizierung wird vom Auftragnehmer regelmäßig überprüft und bestätigt. Diese reicht dem Auftragnehmer als geeignete Maßnahmen aus.

(4) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese Vorort-Kontrolle von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(5) Der Auftragnehmer verpflichtet sich, dem kontrollpflichtigen Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und geeignete Unterlagen vorzulegen. Hieraus resultierende Kosten des Auftragnehmers trägt der Auftraggeber in Höhe der jeweils geltenden Honorarsätze der Dienstleister und der SEWOBE Preislisten.

§ 10 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Grundsätzlich findet die gesamte Kommunikation über das SEWOBE Serviceportal statt.

(2) Bei etwaigen Widersprüchen gehen die Regelungen dieses Auftragsverarbeitungsvertrags den Regelungen des Softwaremietvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so ersetzen die Vertragsparteien innerhalb einer Zeitspanne von max. 4 Wochen die Regelung durch eine rechtlich zulässige Formulierung, die dem ursprünglich Vereinbarten am nächsten kommt. Vorstehendes gilt entsprechend, falls diese Vereinbarung Lücken enthalten sollte.

(3) Es gilt deutsches Recht. Ausschließlicher Gerichtsstand und Erfüllungsort ist Augsburg.

Gelesen und akzeptiert

mbuf
Microsoft Business User Forum e.V.
Werner-von-Siemens-Str. 2
D-64319 Pfungstadt
www.mbuf.de

Ort, Datum: Pfungstadt, 18.05.2018

Organisation: Microsoft Business User Forum e.V. (mbuf)

Verantwortliche(r): Stefan Busch Schatzmeister; Ralph Alkemade Vorstandssprecher

Unterschrift Auftraggeber

Augsburg, den 12.04.2018

SEWOBE
SEWOBE GmbH
Werner-Haas-Str. 8
D - 86153 Augsburg
Tel.: +49 821 455 564 100
Fax: +49 821 455 564 101
E-Mail: info@sewobe.de

Eiko Trausch

Thomas Weishaupt

Unterschrift Auftragnehmer (SEWOBE)

Anlage 1
Technische u. Organisatorische Maßnahmen der SEWOBE

Anlage 1

Technische und organisatorische Maßnahmen gem. Art 32 DSGVO

der

SEWOBE GmbH
Werner Haas Str. 8
86153 Augsburg

Nachfolgend werden die getroffenen technischen und organisatorischen Maßnahmen des Auftragnehmers beschrieben, die zur Umsetzung und Einhaltung der Anforderungen der aktuellen Datenschutzgesetze und Verordnungen, insbesondere Art. 32 DSGVO, eingesetzt werden.

Die technischen und organisatorischen Maßnahmen unterliegen dabei dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftraggeber gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei muss das Sicherheitsniveau der festgelegten Maßnahmen verbessert werden. Wesentliche Änderungen sind mit dem Auftraggeber abzustimmen und zu dokumentieren.

Folgende Maßnahmen werden am Standort der SEWOBE in Augsburg realisiert:

1. Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, dass Unbefugten der räumliche Zutritt zu solchen Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogener Daten verarbeitet oder genutzt werden.

Der Auftragnehmer hat in den Räumen des SEWOBE folgende konkrete Maßnahmen zur Zutrittskontrolle getroffen:

- Die Server befinden sich im Serverraum des Auftragnehmers bzw. in einem Rechenzentrum auf dem Gebiet der Bundesrepublik Deutschland.
- Besucher bzw. Dritte haben Zutritt nur nach Anmeldung zu Räumlichkeiten des Auftragnehmers (Regelung für Firmenfremde)
- Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde)
- Schlüsselregelung (codierte Zugänge)
- Gegenseitige Überwachung (4-Augen-Prinzip)
- Anwesenheitsaufzeichnung anhand Zugangsprotokoll

2. Zugangskontrolle

Ziel der Zugangskontrolle ist es, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden, mit denen die Verarbeitung und Nutzung personenbezogener Daten durchgeführt werden.
Der Zugang zu Datenstationen (PC, Server, Netzkomponenten) erfolgt durch Berechtigungsvergabe und Authentifizierung in allen Systemen. Die Zugangsregelungen umfassen folgende Maßnahmen:

- Passwortvergabe (Klein- und Großbuchstaben, Sonderzeichen, Zahlen, min. 8 Zeichen, regelmäßiger Wechsel, Passworthistorie.

- Rechtezuweisungen sind an Zugangskennungen gebunden (Einteilung nach Administrator, Benutzer etc.)
- Bildschirmsperre bei Abwesenheit mit Passwort-Aktivierung
- Firewall und Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches sind im Einsatz.
- Kontrollierte Vernichtung von Datenträgern (Papier per Shredder)
- Arbeitsanweisung und Bearbeitungsverfahren für Datenerfassungsvorlagen
- Prüf-, Abstimm- und Kontrollsysteme
- Verschlüsselungssysteme
- Zuordnung einzelner Terminals

3. Zugriffskontrolle

Die Maßnahmen zur Zugriffskontrolle müssen darauf gerichtet sein, unerlaubte Tätigkeiten (z.B. unbefugtes lesen, kopieren, verändern oder entfernen) in DV-Systemen außerhalb eingeräumter Berechtigungen zu verhindern.
Der Auftragnehmer hat folgende konkrete Maßnahmen zur Zugriffskontrolle getroffen:

Beim Auftragnehmer ist die Authentifizierung aller Benutzer und Datenstationen im System inkl. Zugangsregelungen und Benutzerberechtigungen durch entsprechende Maßnahmen gewährleistet.

Im Rahmen der Zugriffskontrolle sind folgende Maßnahmen umgesetzt:

- ein schriftliches Berechtigungskonzept wurde erstellt
- ein programmtechnisches Berechtigungskonzept ist eingesetzt
- eine Clear Desk Policy ist vorhanden
- Firewall und Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches sind im Einsatz.
- Regelung der Zugriffsberechtigung
- Verschlüsselung „unterwegs“
- Teilzugriffsberechtigung auf Datenbestände und Funktionen

4. Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Der Auftragnehmer hat folgende konkrete Maßnahmen zur Weitergabekontrolle getroffen:

Die Datenübertragung vom Auftraggeber an den Auftragnehmer kann auf unterschiedliche Arten erfolgen und muss zwischen den Partnern abgestimmt werden. Der Auftragnehmer unterstützt gängige sichere Varianten. Verschlüsselte Tunnelung von Verbindungen oder sichere Übertragung via VPN.

- Verbot der Nutzung privater Datenträger am Arbeitsplatz
- Feststellung befugter Personen
- Gegenseitige Überwachung (4-Augen-Prinzip)
- Plausibiltätsprüfung

5. Eingabekontrolle

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass nachträglich die näheren Umstände der Dateneingabe überprüft und festgestellt werden können.

Der Auftragnehmer hat folgende konkrete Maßnahmen zur Eingabekontrolle getroffen:

- Dem Auftraggeber werden vom Auftragnehmer Zugangsregelungen und Benutzerberechtigungen vorgegeben, wodurch die Identifizierung aller Benutzer und Datenstationen im System möglich ist.
- Auf den Servern des Auftragnehmers bzw. in den Programmen werden Änderungen protokolliert.
- Die Eingabekontrolle in Datenbanksystemen erfolgt im Rahmen der mit den Datenbanksystemen gelieferten Standardverfahren, die je nach Datenbanksystem bis zur Erfassung aller Eingaben umfassen kann.

6. Auftragskontrolle

Ziel der Auftragskontrolle ist es sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Der Auftragnehmer hat folgende konkrete Maßnahmen zur Auftragskontrolle getroffen:

- Jeglicher Aktivität liegt ein Auftrag des auftragsberechtigten Kunden zugrunde. Im Minimum gilt ein bestehendes Vertragswerk.
- Formalisierung der Auftragserteilung
- Kontrolle des Auftragnehmers bezüglich der Einhaltung des Vertrages
- Sorgfältige Auswahl der Subunternehmer.
- Vereinbarung der Datenschutzmaßnahmen in mindestens gleichem Umfang wie mit dem Auftraggeber

7. Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es sicherzustellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Der Auftragnehmer hat folgende konkrete Maßnahmen zur Verfügbarkeitskontrolle getroffen:

- Es ist eine Notfallplanung vorhanden und in Notfallkonzepten dokumentiert. Die Funktionsfähigkeit dieser Konzepte wird in regelmäßigen Abständen (meist jährlich) geprüft. Die Notfallpläne werden einem regelmäßigen Prüf- und Verbesserungsprozess unterzogen.
- Es ist ein Unterbrechungsfreie Stromversorgung (USV) im Einsatz.
- Regelmäßige Sicherungskopien
- Back-up Lösungen

8. Zweckbindungskontrolle

Ziel der Zweckbindungskontrolle ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Der Auftragnehmer hat folgende konkrete Maßnahmen zur Zweckbindungskontrolle getroffen:

- Die Verarbeitung der Daten erfolgt nur im Rahmen der von SEWOBE zur Verfügung gestellten Software zur Mitgliederverwaltung auf Servern des Auftragnehmers bzw. Servern der beauftragten Subunternehmer.
- Art und Umfang der erfassten Daten liegen ausschließlich im Verantwortungsbereich des Auftraggebers.

Ende der technischen und organisatorischen Maßnahmen