Vereinbarung über die Auftragsverarbeitung

Zwischen dem / der

Firmenname

Straße / Hausnummer

PLZ und Ort

Land

Name des Ansprechpartners/der Ansprechpartnerin

- Verantwortlicher -

- nachstehend Auftraggeber genannt -

und der

ATOSS Aloud GmbH

Rosenheimer Str. 141 h

81671 München

- Auftragsverarbeiter -

- nachstehend Auftragnehmer genannt -

- nachstehend einzeln oder gemeinsam auch Parteien genannt -

Inhaltsverzeichnis:

Anlagen:

Präambel

(1) Gesetzliche Grundlage

Die nachfolgende Vereinbarung zur Auftragsdatenverarbeitung bzw. Auftragsverarbeitung (nachfolgend einheitlich: Auftragsverarbeitung) dient als Grundlage zur Erfüllung der gesetzlichen Bestimmungen zum Datenschutz im Hinblick auf die bestehenden oder zukünftigen Vertragsverhältnisse der Parteien über die Bereitstellung der Crewmeister-Softwarelösungen als Software-as-a-Service über verschiedene Zugangswege (z.B. Apps, Webbrowser etc.) sowie den Support betreffend die dem Auftraggeber vom Auftragnehmer zur Nutzung bereitgestellten Software-Lösungen durch den Auftragnehmer (nachfolgend: Leistungsvereinbarungen). Die gesetzlichen Grundlagen bilden ab dem 25.05.2018 die Bestimmungen der EU-Datenschutzgrundverordnung (nachfolgend: DS-GVO) und des Bundesdatenschutzgesetzes in der ab dem 25.05.2018 geltenden Fassung (nachfolgend: BDSG n.F.). Bis dahin richtet sich die Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber in dessen Auftrag nach den Bestimmungen des Bundesdatenschutzgesetzes in der aktuell gültigen Fassung (nachfolgend: BDSG a.F.).

(2) Vertragliche Grundlage

Soweit der Auftragnehmer personenbezogene Daten der Beschäftigten des Auftraggebers (nachfolgend: Auftragsdaten) verarbeitet, gelten hierfür die Bedingungen der vorliegenden Vereinbarung über die Auftragsverarbeitung. Für die in dieser Vereinbarung verwendeten Begriffe wie z. B. „personenbezogene Daten“, „Verarbeitung“ oder „Pseudonymisierung“ wird auf Art. 4 DS-GVO verwiesen.

(3) Verantwortlichkeit des Auftraggebers

Der Auftraggeber ist auch im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer, für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch den Auftragnehmer sowie für die Wahrung der Rechte der Betroffenen, allein verantwortlich („Verantwortlicher“ i.S.v. Art. 4 Nr. 7 DS-GVO).

§ 1 - Gegenstand und Dauer der Verarbeitung

(1) Gegenstand

Der Auftragnehmer stellt dem Auftraggeber die Crewmeister-Software-Lösungen als Software-as-a-Service über verschiedene Zugangswege (z.B. Apps, Webbrowser etc.) bereit und unterstützt den Auftraggeber bei der Nutzung der Software (Support). Da die Datenhaltung der Crewmeister-Software-Lösungen beim Auftragnehmer bzw. bei dessen Unterauftragnehmern erfolgt, umfassen diese Leistungen naturgemäß auch Sachverhalte der Auftragsverarbeitung. In all diesen Sachverhalten verarbeitet der Auftragnehmer personenbezogene Daten des Auftraggebers ausschließlich im Auftrag, nach Weisung und im Interesse des Auftraggebers.

(2) Dauer

Die Laufzeit dieses Auftrags entspricht der Dauer der Zusammenarbeit der Parteien auf Basis der jeweiligen Leistungsvereinbarungen. Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen diese Vereinbarung vorliegt oder wenn der Auftragnehmer vereinbarungsgemäße Kontrollen durch den Auftraggeber ganz oder teilweise verweigert.

§ 2 - Auftragsinhalt im Einzelnen

(1) Art und Zweck der Verarbeitung

(a) Art

Auftraggeber und Auftragnehmer stehen in einer geschäftlichen Beziehung, in dessen Rahmen der Auftragnehmer Leistungen zur Auftragsverarbeitung für den Auftraggeber erbringt. Diese umfassen folgende Arten der Verarbeitung:

- Zurverfügungstellung der Software-Lösungen von Crewmeister im Rahmen von Software-as-a-Service über verschiedene Zugangswege (z.B. Apps, Webbrowser etc.), in diesem Rahmen Speicherung, Verarbeitung und Zurverfügungstellung der vom Auftraggeber bzw. dessen Mitarbeitern erfassten personenbezogene Daten wie z.B. Arbeitszeiten sowie darauf basierend verarbeitete personenbezogene Daten wie z.B. kumulierte Zeitkonten.
- Support-Leistungen betreffend die vom Auftragnehmer als Software-as-a-Service zur Nutzung zur Verfügung gestellten Software-Lösungen von Crewmeister (insbesondere zur Unterstützung bei der Suche nach Ursachen für vom Auftraggeber gemeldete Fehlfunktionen; Fehlerbehebung bei der Datenübergabe per Schnittstelle an Fremdsysteme (z.B. Lohn und Gehalt) sowie bei der Datenerfassung mit den Crewmeister-Software-Lösungen).

In allen Fällen ist eine lesende und schreibende Zugriffsmöglichkeit des Auftragnehmers auf die in der Crewmeister-Datenbank befindlichen Auftragsdaten gegeben.

(b) Zweck

Zweck der Verarbeitung ist die Gewährleistung der Funktionalität und ggf. der Aktualität der dem Auftraggeber vom Auftragnehmer zur Nutzung zur Verfügung gestellten Software-Lösungen.

(2) Kategorien der personenbezogenen Daten

Der Auftragnehmer verarbeitet im Rahmen dieses Vertragsverhältnisses folgende Kategorien personenbezogener Daten des Auftraggebers (variabel je nach Nutzungsumfang des Kunden):

- Stammdaten:
    - Personalnummer
    - Anrede, Name
    - Geburtsdatum
    - Mitarbeiterkategorie
    - Sonstige vertragsrelevante Daten wie Eintritts-, Austritts- Umgruppierungsdaten
    - Vereinbarungen zur Arbeitszeit
    - Kontaktdaten (wie Anschrift, Email, Telefonnummern)
    - Mitarbeiterfoto
    - Sonstige organisatorische Merkmale
- Informationen über Zugehörigkeit zu bestimmten Regionen / Ländern / Sprachen
- Informationen über Arbeitsorte und Wegezeiten
- Informationen über Vorgesetzten-, Mitarbeiter-, und Stellvertreterbeziehungen
- Sonstige personenbezogene Daten, die von Endanwendern in frei definierbaren Feldern gespeichert werden
- Informationen über Qualifikationen und Ausbildungsmaßnahmen
- Informationen über Zeitkonten
- Informationen über einzelvertragliche, tarifliche und sonstige Vergütungs-, Urlaubs- und Freizeitansprüche von Mitarbeitern:
    - generelle Vereinbarungen
    - historische und aktuelle tatsächliche Werte und Salden
- Informationen über geplante und tatsächliche Abwesenheiten
- Informationen über Buchungen inkl. Uhrzeit und Ort der Buchung
- Informationen über tatsächliche Anwesenheits-, (Ruf-)Bereitschafts- und Arbeitszeiten

- Informationen über Zugehörigkeit zu Organisationseinheiten, Projekten, Aufträgen, Kostenstellen, Arbeitsplätzen etc. und den dafür geleisteten Zeiten
- Manuelle Anmerkungen zu Stamm- und Bewegungsdaten
- Systemseitige Warnungen und Fehlermeldungen bei Abweichungen von Vorgaben oder Regeln
- Informationen über vertragliche und planerische Verfügbarkeit von Mitarbeitern
- Informationen über Planungswünsche von Mitarbeitern
- Informationen über Einsatzplanung von Mitarbeitern und tatsächlich geleistete Arbeitszeiten
- Informationen über Planänderungen
- Informationen über Schichttausch-Vorgänge von Mitarbeitern
- Informationen über Leistungsprofile von Mitarbeitern
- Anträge für Abwesenheiten inkl. Genehmigungsverlauf und -stand
- Anträge für arbeitszeit- oder dienstplanungsrelevante Vorgänge inkl. Genehmigungsverlauf und -stand
- Anstehende und erledigte Aufgaben
- Informationen über vom System versandte E-Mail- und SMS-Benachrichtigungen
- Systemzugangsinformationen
- Informationen über Berechtigungen für bestimmte Objekte und Interaktionen als Benutzer des Systems
- Zuletzt verwendete Systemeinstellungen und Präferenzen
- Angemeldete Systembenutzer
- Anmeldeversuche
- Protokolle über Benutzerinteraktionen, die Daten im System verändern.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Beschäftigte i. S. d. § 3 Abs. 11 BDSG a.F. bzw. i. S. d. § 26 Abs. 8 BDSG n.F.

(4) Sachliche und örtliche Beschränkung der Verarbeitung

(a) Sachlich

Eine über diese Vereinbarung hinausgehende Verarbeitung von Auftragsdaten ist dem Auftragnehmer nicht gestattet. Eine Verarbeitung für andere Zwecke, insbesondere die Weitergabe von Auftragsdaten an Dritte, ist nicht zulässig. Der Auftragnehmer ist verpflichtet, die Auftragsdaten verschiedener Kunden (logisch) getrennt zu verarbeiten.

(b) Örtlich

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union (nachfolgend: EU), in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (nachfolgend: EWR) und/oder Mithilfe von Dienstleistern, die unter dem EU/Schweiz-US-Privacy-Shield zertifiziert sind, in den Vereinigten Staaten von Amerika (nachfolgend: USA) statt. Auch sofern die Datenverarbeitung in den USA stattfindet, findet sie stets auf Grundlage einer den Anforderungen der Datenschutz-Grundverordnung entsprechenden Auftragsverarbeitungsvereinbarung zwischen der ATOSS Aloud GmbH als Auftragnehmer und dem Dienstleister als Unterauftragnehmer des Auftragnehmers statt.

Dessen ungeachtet kann der Auftraggeber die personenbezogenen Daten auch außerhalb der EU/des EWR über die von Crewmeister offerierten Nutzungswege aufrufen. Hierbei werden die Daten an die Client-Geräte des Auftraggebers unabhängig von dessen Standort übermittelt, also ggf. auch außerhalb der EU bzw. des EWR.

Der Auftragnehmer wird die vertraglich vereinbarte Leistung ggf. von den in Anlage 2 vereinbarten Leistungsstandorten aus durch die genehmigten Unterauftragnehmer (siehe § 6) erbringen. Im Falle von Änderungen wird dem Auftraggeber die jeweils aktuelle Fassung der Anlage 2 auf geeignete Weise zur Verfügung gestellt, z.B. auf einem über die Website des Auftragnehmers zugänglichen Online-Portal.

§ 3 - Technische und organisatorische Maßnahmen

(1) Gewährleistung der Datensicherheit

Der Auftragnehmer hat die Grundsätze ordnungsgemäßer Datenverarbeitung zu beachten und ihre Einhaltung zu überwachen (vgl. Art. 5 DS-GVO). Er versichert, dass er die Regelungen der Art. 28 Abs. 3 lit. c, 32 DS-GVO einhält. Er hat hierzu angemessene Maßnahmen der Datensicherheit getroffen und gewährleistet unter fortlaufender Vornahme ggf. erforderlicher Anpassungen ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Hierbei werden der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen fortlaufend berücksichtigt (vgl. zu den Einzelheiten die Anlagen 1A und 1B).

(2) Dokumentation und Vorlage der Maßnahmen

Der Auftragnehmer hat die technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung mit Blick auf die konkrete Auftragsdurchführung zu dokumentieren und dem Auftraggeber diese Dokumentation zur Prüfung zur Verfügung zu stellen (siehe Anlagen 1A und 1B). Mit Abschluss dieser Vereinbarung werden die dokumentierten Maßnahmen Grundlage der

Auftragsverarbeitung. Soweit die Prüfung des Auftraggebers unter Berücksichtigung der in diesem § 3 Abs. (1) genannten Kriterien einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen sind zu dokumentieren und dem Auftraggeber auf geeignete Weise zur Verfügung zu stellen, z.B. auf einem über die Website des Auftragnehmers zugänglichen Online-Portal.

(3) Aktueller Stand der Technik

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dieser Vereinbarung festgelegten Maßnahmen nicht unterschritten werden.

§ 4 - Weisungsbefugnis

(1) Dokumentierte Weisung

Der Auftraggeber hat das Recht, dem Auftragnehmer Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Der Auftraggeber entscheidet allein und ausschließlich über die Zwecke und Mittel der Verarbeitung der Auftragsdaten. Der Auftragnehmer darf die Auftragsdaten nur nach dokumentierter Weisung des Auftraggebers verarbeiten, es sei denn, der Auftragnehmer ist gesetzlich zur Verarbeitung dieser Daten verpflichtet.

(2) Bestimmtheit und Form der Weisung

Weisungen sind bestimmt zu erteilen (Gebot der Weisungsklarheit). Weisungen können schriftlich, in Textform oder in Eilfällen auch mündlich erteilt werden. Mündliche Weisungen muss der Auftraggeber unverzüglich schriftlich oder in Textform bestätigen.

(3) Benachrichtigung bei Rechtswidrigkeit

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung sei rechtswidrig. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(4) Rechte der betroffenen Personen

Auskünfte an von der Auftragsverarbeitung betroffene Personen oder an Dritte darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit eine betroffene

Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(5) Auftragsfremde Weisungen

Für die Ausführung von Weisungen des Auftraggebers, die über die in dieser Vereinbarung geregelten Leistungen hinausgehen, kann der Auftragnehmer eine gesonderte Vergütung beanspruchen.

(6) Regress

Sollte der Auftragsverarbeiter infolge der Umsetzung einer rechtswidrigen Weisung einem begründeten Haftungsanspruch ausgesetzt sein, kann er sich insoweit beim Verantwortlichen schadlos halten.

§ 5 - Verpflichtung zur Vertraulichkeit

(1) Daten- und Fernmeldegeheimnis

Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu Auftragsdaten hat, sind zur Vertraulichkeit verpflichtet, insbesondere gemäß den Bestimmungen des § 5 BDSG a.F. bzw. des § 53 BDSG n.F. sowie des § 88 TKG. Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung dieser Vereinbarung fort.

(2) Unterweisung aller zur Auftragsverarbeitung eingesetzten Personen

Der Auftragnehmer stellt durch geeignete Maßnahmen wie insbesondere regelmäßige Schulungen zum Datenschutz sicher, dass die ihm unterstellten und zur Verarbeitung von Auftragsdaten befugten Personen mit den einschlägigen Bestimmungen zum Datengeheimnis und Fernmeldegeheimnis vertraut sind.

§ 6 - Beauftragung von Unterauftragnehmern

(1) Begriff des Unterauftragnehmers

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer etwa als Telekommunikationsleistungen, Post- / Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Unterlagen und Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit,

Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und rechtskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Voraussetzungen der Zulässigkeit der Beauftragung

Der Auftragnehmer darf Unterauftragnehmer im Rahmen der Auftragsverarbeitung nur unter Beachtung nachfolgender Voraussetzungen beauftragen. Hinsichtlich der mit dem Auftragnehmer i.S.v. §§ 15 ff. AktG verbundenen Unternehmen gilt die Zustimmung des Auftraggebers mit Abschluss dieser Vereinbarung als erteilt; diese sind in Anlage 2 zu dieser Vereinbarung aufgeführt.

(a) Die Auslagerung auf Unterauftragnehmer oder der Wechsel der bestehenden Unterauftragnehmer sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf (andere) Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt,
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO zugrunde gelegt wird, die mindestens den Regelungen dieser Vereinbarung entspricht.

(b) Bei einer Leistungserbringung außerhalb Deutschlands aus Ländern, die Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, wird der Auftraggeber sein Einverständnis hinsichtlich der Zustimmung zur Verlagerung oder des Einsatzes eines Unterauftragnehmers nicht unbillig verweigern, wenn sich diese Verlagerung nicht negativ auf den Datenschutz auswirkt und der Auftragnehmer dem Auftraggeber vorab Details zur Verlagerung und der vom neuen Standort erbrachten Leistungen schriftlich oder in Textform mitgeteilt hat.

Eine Auftragsverarbeitung außerhalb der EU bzw. des EWR ist ausgeschlossen.

(3) Geltung der Bestimmungen dieser Vereinbarung auch für Unterauftragnehmer

Sämtliche in dieser Vereinbarung vom Auftragnehmer übernommenen Verpflichtungen sind auch allen Unterauftragnehmern in gleicher Weise aufzuerlegen. Der Auftragnehmer hat die Einhaltung dieser Pflichten der Unterauftragnehmer regelmäßig zu überprüfen. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber gegenüber Unterauftragnehmern die gleichen Kontrollrechte hat wie gegenüber dem Auftragnehmer selbst.

Die Weitergabe von Auftragsdaten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden im Rahmen der Auftragsverarbeitung sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

§ 7 - Pflichten und Rechte des Auftraggebers; Unterstützung des Auftraggebers durch den Auftragnehmer

Der Auftraggeber ist zur Wahrung der Rechte der betroffenen Person (Art. 12 ff. DS-GVO bzw. §§ 32 ff. BDSG n.F.), zur Ergreifung technischer und organisatorischer Maßnahmen, zur Meldung und Benachrichtigung bei Datenpannen, zur Zusammenarbeit mit der Aufsichtsbehörde (Art. 32 bis 36 DS-GVO) sowie zur Qualitätssicherung (Art. 28 Abs. 1 DS-GVO) verpflichtet. Der Auftraggeber trägt in seinem Verantwortungsbereich dafür Sorge, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten geschaffen werden. Bei der Einhaltung der Pflichten unterstützt der Auftragnehmer den Auftraggeber. In diesem Zusammenhang stellt er ihm sämtliche Informationen bereit, soweit der Auftraggeber über diese Informationen nicht selbst verfügt. Der Auftragnehmer ist nicht verpflichtet, Informationen zum Zweck der Unterstützung zu beschaffen, über die er seinerseits nicht verfügt. Der Auftragnehmer unterstützt den Auftraggeber wie folgt:

(1) Wahrung der Rechte der betroffenen Personen

(a) Die Wahrung der Rechte der betroffenen Personen obliegt dem Auftraggeber. Soweit erforderlich, unterstützt der Auftragnehmer den Auftraggeber im Falle der Ausübung von Rechten durch die betroffenen Personen.

(b) Der Auftraggeber hat für die Verarbeitung besonderer Kategorien personenbezogener Daten i. S. d. § 22 Abs. 1 BDSG n.F. angemessene und spezifische Maßnahmen zur Wahrung der Rechte der betroffenen Personen vorzusehen. Der Auftragnehmer unterstützt den Auftraggeber hierbei u. a. durch Ergreifung angemessener Maßnahmen i. S. d. § 22 Abs. 2 BDSG n.F. im Rahmen der Auftragsverarbeitung.

(2) Technische und organisatorische Maßnahmen

Der Auftragnehmer unterstützt den Auftraggeber bei der Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

Der Auftraggeber hat hierbei insbesondere in geeigneter und dem Schutzbedarf angemessener Form sicherzustellen, dass die vom Auftragnehmer bereitgestellten Software-Lösungen sowie die damit verbundenen technischen Schnittstellen gegen unbefugten Zugriff gesichert werden (z.B. durch Vergabe lediglich temporär gültiger Zugangskennungen und / oder regelmäßige Passwortänderungen und / oder Beschränkungen des zugriffsberechtigten IP-Adress-Bereichs oder andere vergleichbare Maßnahmen).

(3) Meldepflicht und Benachrichtigungspflicht

Im Falle der Verletzung des Schutzes von Auftragsdaten durch den Auftragnehmer ist der Auftragnehmer verpflichtet, den Auftraggeber im Hinblick auf dessen

- Meldepflicht gegenüber der zuständigen Aufsichtsbehörde und

- Benachrichtigungspflicht gegenüber den betroffenen Personen

zu unterstützen. Im Fall einer schwerwiegenden Betriebsstörung, bei Verdacht auf Datenschutzverletzungen oder bei Verletzungen dieser Vereinbarung, gleich ob diese durch den Auftraggeber, einen Dritten oder den Auftragnehmer verursacht wurden, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang der betroffenen Auftragsdaten zu informieren. Dem Auftraggeber sind sämtliche relevante Informationen zur Erfüllung der Meldepflicht gegenüber der Aufsichtsbehörde unverzüglich zur Verfügung zu stellen.

(4) Zusammenarbeit mit der Aufsichtsbehörde

Die Parteien arbeiten mit der zuständigen Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben im Rahmen des Erforderlichen gemäß nachfolgenden Grundsätzen zusammen.

(a) Kontrollhandlungen beim Auftragnehmer oder Auftraggeber

(aa) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung von Auftragsdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(bb) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(b) Datenschutz-Folgenabschätzung

Soweit eine gesetzliche Pflicht des Auftraggebers zur Erstellung einer Datenschutz-Folgenabschätzung besteht, unterstützt ihn der Auftragnehmer bei der Vornahme der Datenschutz-Folgenabschätzung sowie bei einer etwaig erforderlichen vorherigen Konsultation der Aufsichtsbehörde im ggf. erforderlichen Umfang. Dies beinhaltet insbesondere die Übermittlung ggf. erforderlicher Angaben bzw. die Offenlegung ggf. erforderlicher Dokumente auf entsprechendes Verlangen des Auftraggebers.

(5) Qualitätssicherung

(a) Überprüfungen

Der Auftraggeber hat das Recht, sich durch Stichprobenkontrollen, die mit einer angemessenen Vorlaufzeit beim Auftragnehmer bzw. dessen Unterauftragnehmern anzumelden sind, von der Einhaltung der gesetzlichen und in dieser Vereinbarung übernommenen Verpflichtungen des Auftragnehmers bzw. von dessen Unterauftragnehmern in dessen Geschäftsbetrieb zu dessen Geschäftszeiten zu überzeugen. Er kann diese Überprüfungen selbst durchführen oder durch von ihm zu benennende, auf Vertraulichkeit nach § 5 dieser Vereinbarung zu verpflichtende, Dritte auf seine Kosten durchführen lassen. Dritte in diesem Sinne dürfen keine Vertreter von Wettbewerbern des Auftragnehmers sein.

Der Auftragnehmer kann der Überprüfung durch einen externen Prüfer widersprechen, wenn der vom Auftraggeber ausgewählte Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(b) Dokumentation

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO im Rahmen der Auftragsverarbeitung überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Dokumentation der technischen und organisatorischen Maßnahmen zur Verfügung zu stellen.

Der Nachweis der Dokumentation der technischen und organisatorischen Maßnahmen kann dabei insbesondere auch durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit erfolgen.

(c) Datenschutzbeauftragter

Der Auftragnehmer sichert ferner zu, seinen gesetzlichen Verpflichtungen im Hinblick auf die ggf. erforderliche Bestellung eines Datenschutzbeauftragten nachzukommen. Insoweit wird die Bestellung eines Datenschutzbeauftragten sichergestellt, dem die erforderliche Zeit zur Erledigung

seiner Aufgaben gewährt wird und der über eine nachweisbare Fachkunde und die erforderliche Zuverlässigkeit gemäß den gesetzlichen Bestimmungen verfügt.

(6) Sonstige Unterstützungsleistungen

Für weitere Unterstützungsleistungen, die nicht in den Leistungsvereinbarungen enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine gesonderte Vergütung beanspruchen.

§ 8 - Löschung oder Rückgabe nach Abschluss der Verarbeitung

(1) Wahlrecht

Nach Aufforderung durch den Auftraggeber – spätestens 12 Monate nach vollständiger Sperrung des Zugangs – hat der Auftragnehmer auf eigene Kosten sämtliche in seinen Besitz gelangten Unterlagen, Datenträger, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Auftragsverarbeitung stehen, dem Auftraggeber nach dessen Wahl zurückzugeben oder datenschutzgerecht zu löschen bzw. zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Kopien der Auftragsdaten

Kopien oder Duplikate der Auftragsdaten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung sowie zur Fehlerbehebung erforderlich sind, die Fertigung und Zwischenspeicherung von Screenshots von Auftragsdaten zum Zwecke der Fehleranalyse sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Aufbewahrungsfristen

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(4) Kosten

Zusätzliche Kosten, die durch von diesem § 8 Abs. (1) abweichende bzw. darüberhinausgehende Weisungen des Auftraggebers entstehen, hat der Auftraggeber zu tragen.

§ 9 - Haftung

Der Auftragnehmer haftet gegenüber dem Auftraggeber für schuldhafte Verletzungen dieser Vereinbarung nach den gesetzlichen Bestimmungen. Der Auftragnehmer haftet gegenüber dem Auftraggeber für das Verschulden eines von ihm beauftragten Unterauftragnehmers wie für eigenes Verschulden.

§ 10 - Schlussbestimmungen

(1) Ersetzungsklausel; Änderungen und Ergänzungen

(a) Diese Vereinbarung tritt mit ihrer Unterzeichnung durch beide Parteien in Kraft und ersetzt mit ihrem Inkrafttreten in ihrem Anwendungsbereich sämtliche etwaig bestehenden Vereinbarungen zur Auftrags(daten)verarbeitung zwischen den Parteien.

(b) Alle Änderungen und Ergänzungen zu dieser Vereinbarung sowie alle Nebenabreden bedürfen zu ihrer Wirksamkeit der Schriftform oder Textform.

(2) Nichtanwendbarkeit der Allgemeinen Geschäfts- / Einkaufsbedingungen des Auftraggebers

Es besteht zwischen den Parteien Einigkeit darüber, dass "Allgemeine Geschäftsbedingungen" und / oder „Allgemeine Einkaufsbedingungen“ des Auftraggebers auf diese Vereinbarung keine Anwendung finden.

(3) Ausschluss des § 273 BGB

Die Einrede des Zurückbehaltungsrechts gemäß § 273 BGB wird hinsichtlich der verarbeiteten Auftragsdaten und der zugehörigen Datenträger ausgeschlossen.

(4) Verpflichtung zur Vertraulichkeit

Die Parteien verpflichten sich, alle im Rahmen der Auftragsverarbeitung erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen sowie von Maßnahmen zur Datensicherheit der jeweils anderen Partei vertraulich zu behandeln. Betriebs- und Geschäftsgeheimnisse sind alle auf das Unternehmen einer der Parteien bezogenen Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung die betreffende Partei ein berechtigtes Interesse hat. Maßnahmen zur Datensicherheit sind alle technischen und organisatorischen Maßnahmen, die eine Partei im Sinne der Anlagen 1A bzw. 1B zu dieser Vereinbarung getroffen hat. Diese Geheimhaltungspflicht besteht nach Beendigung dieses Vertrags fort.

(5) Verpflichtung zur Information im Fall der Gefährdung der Auftragsdaten

Im Fall der Gefährdung der Auftragsdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter, ist der Auftragnehmer verpflichtet, den Auftraggeber darüber unverzüglich zu informieren.

(6) Gerichtsstand

Alleiniger Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist, vorbehaltlich eines etwaigen ausschließlichen gesetzlichen Gerichtsstandes, München.

(7) Anwendbares Recht

Diese Vereinbarung unterliegt deutschem Recht.

(8) Salvatorische Klausel

Sollten einzelne Teile dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, wird hierdurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Parteien verpflichten sich, anstelle der unwirksamen oder undurchführbaren Bestimmung eine wirksame und durchführbare Bestimmung zu vereinbaren, die dem ursprünglich gewollten Sinn und Zweck der unwirksamen oder undurchführbaren Bestimmung am nächsten kommt. Dies gilt im Falle einer Regelungslücke entsprechend.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
(Unterschrift Auftraggeber)	(Unterschrift Auftragnehmer)

Anlage 1 - Technische und organisatorische Maßnahmen der ATOSS Konzerngesellschaften

A. Inhaltsverzeichnis

B. Hinweise zum Aufbau

Die Begrifflichkeiten der vorliegenden Liste an technischen und organisatorischen Maßnahmen sind Art. 32 Abs. 1 DS-GVO sowie § 22 Abs. 2 BDSG n.F. entnommen. Den Rahmen bilden die in der Liste genannten Begriffe der DS-GVO:

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit und Belastbarkeit,
- Wiederherstellung der Verfügbarkeit der personenbezogenen Daten und des Zugangs zu ihnen sowie
- Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Die Begrifflichkeiten des § 64 Abs. 3 BDSG n.F. sind gesetzlich nur dann zwingend zu berücksichtigen, wenn es sich um Verantwortliche oder Verarbeiter als öffentliche Stellen i.S.d. § 45 BDSG n.F. handelt. Der besseren Untergliederung wegen wurden die Begriffe jedoch auch der vorliegenden Liste zugrunde gelegt:

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle

Stand: 01.08.2019

- Eingabekontrolle
- Transportkontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit

C. Checkliste

I.	**Vertraulichkeit**
I.1	**Zugangskontrolle**
I.1.1	**Bürogebäude und Arbeitsplätze**
I.1.1.0	*Von folgenden **Geschäftsstellen und Konzerngesellschaften** (ggf. nachfolgend gemeinsam: alle Standorte) wird ggf. auch auf Auftragsdaten zugegriffen:* Unternehmenssitz ATOSS Aloud GmbH Rosenheimer Str. 141 h 81671 München Weitere ATOSS-Konzerngesellschaft (i.S.v. §§ 15 ff. AktG) in Deutschland: Unternehmenssitz: ATOSS Software AG Rosenheimer Str. 141 h 81671 München Geschäftsstellen Deutschland: ATOSS Software AG Pfalzburger Straße 42 10717 Berlin ATOSS Software AG Robert-Bosch-Straße 14 40668 Meerbusch ATOSS Software AG Campus Carré Herriotstraße 8 60528 Frankfurt am Main ATOSS Software AG Osterbekstraße 90b 22083 Hamburg ATOSS Software AG Eichwiesenring 1/1 70567 Stuttgart

	Geschäftsstelle Niederlande: ATOSS Software AG Newtonlaan 115 3584 BH Utrecht Weitere ATOSS-Konzerngesellschaft (i.S.v. §§ 15 ff. AktG) in Deutschland: ATOSS CSD Software GmbH Rodinger Straße 19 93413 Cham ATOSS-Konzerngesellschaft (i.S.v. §§ 15 ff. AktG) in Österreich: ATOSS Software Ges.m.b.H. Ungargasse 64-66, Stiege 3, Top 503 1030 Wien ATOSS-Konzerngesellschaft (i.S.v. §§ 15 ff. AktG) in der Schweiz: ATOSS Software AG Badenerstrasse 549 8048 Zürich ATOSS-Konzerngesellschaft (i.S.v. §§ 15 ff. AktG) in Rumänien: SC ATOSS Software SRL Bd. Liviu Rebreanu Nr. 76-78 300755 Timisoara
I.1.1.1	*Die Büroräume befinden sich jeweils in folgenden **Etagen**:* München: im 5. bis 9. OG Berlin: im 2. OG Stuttgart: im 1. OG Frankfurt: im EG Hamburg: im 10. OG Meerbusch: im 1. und 2. OG Utrecht: im 2. OG Cham: im 1. OG Wien: im 5.OG Zürich: im 1. OG Timisoara: im EG, 1. und 2. OG
I.1.1.2	*Es wird ein **Besucherbuch** bezogen auf das Rechenzentrum bzw. auf die Server-Räume geführt:* ☑ Ja ☐ Nein
I.1.1.3	*Folgende Gebäude / Büroräume sind mit einer Einbruchmeldeanlage (**EMA**) ausgestattet:* München: ☑ Ja ☐ Nein Das Gebäude der Firmenzentrale wird von 22:00 Uhr bis 07:00 Uhr durch eine EMA gesichert. Auf allen fünf Etagen befinden sich Bewegungsmelder, Überfallmelder und Videokameras. Sämtliche Fenster sind alarmgesichert. Die Kameras zeichnen täglich zwischen 19:30 Uhr und 07:00 Uhr auf. Auf einem Monitor an der Rezeption können die

	Kamerabilder verfolgt werden. Sämtliche Alarmanlagen in den Geschäftsstellen und Konzerngesellschaften des Auftragnehmers sind vds-konform. Berlin: ☐ Ja ☑ Nein Stuttgart: ☑ Ja ☐ Nein Das Büro wird von 22:00 Uhr bis 07:00 Uhr durch eine EMA gesichert. Frankfurt: ☐ Ja ☑ Nein Hamburg: ☑ Ja ☐ Nein Das Büro wird von 22:00 Uhr bis 06:00 Uhr durch eine EMA gesichert. Im Büro befinden sich zwei Bewegungsmelder. Die Eingangstür ist durch eine EMA gesichert. Die Fluchttür ist durch ein EMA-gesichertes Panikschloss gesichert. Die zweimal im Jahr durchgeführte Wartung erfolgt durch einen Anbieter von Sicherheitstechnik, welcher durch einen Wachdienst unterstützt wird. Die Sicherheit des gesamten Bürokomplexes wird von einem weiteren Wachdienst gewährleistet. Meerbusch: ☑ Ja ☐ Nein Das Büro wird von 22:00 Uhr bis 05:00 Uhr durch eine EMA gesichert. Utrecht: ☑ Ja ☐ Nein Das Büro wird von 18:00 Uhr bis 07:30 Uhr durch eine EMA gesichert. Cham: ☑ Ja ☐ Nein Das Büro wird durch eine EMA gesichert, die zwischen Arbeitsende und Arbeitsbeginn manuell eingeschaltet wird. Wien: ☑ Ja ☐ Nein Das Büro wird durch eine EMA gesichert von 18.00 Uhr bis 08.00 Uhr. Im Büro befinden sich fünf Bewegungsmelder. Zusätzlich wird das Büro zwischen 22.00 Uhr und 23.00 Uhr nochmals durch einen Wachdienst kontrolliert. Das Bürogebäude wird ebenfalls durch einen Wachdienst gesichert. Zürich: ☐ Ja ☑ Nein Timisoara: ☑ Ja ☐ Nein Das gesamte Bürogebäude wird von 21:00 Uhr bis 08:00 Uhr durch eine EMA gesichert. Zwischen 19:00 Uhr und 21:00 Uhr ist die Überwachung zusätzlich durch einen Wachdienst gesichert. Auf allen drei Etagen und im Untergeschoss befinden sich Bewegungsmelder und Videokameras. Bei entdeckter Bewegung zeichnen die Kameras täglich rund um die Uhr auf. Auf einem Monitor an der Rezeption können die Kamerabilder verfolgt werden.
I.1.1.4	*Folgende **Stellen** werden informiert, wenn die EMA einen Alarm aussendet:* München, Stuttgart, Hamburg, Meerbusch: Beauftragter Wachdienst und ein ereignisspezifisch definierter Personenkreis. Utrecht: Empfangsrezeption im Gebäude, anschließend der Standortverantwortliche. Cham: Vermieter und Gebäudeverwaltung. Wien: Standortverantwortlicher und Teamassistenz. Zürich: Keine EMA vorhanden. Timisoara: Beauftragter Wachdienst und interner Sicherheitsbeauftragter.
I.1.1.5	*Folgende Gebäude / Büroräume verfügen über ein **elektronisches Schließsystem**:*

	München: ☑ Ja ☐ Nein Allerdings nur der Eingang zu den einzelnen Trakteinheiten. Pro Etage gibt es zwei Zugänge. Bei Scharf- oder Unscharfschaltung wird die jeweilige andere Tür ebenfalls scharf oder unscharf geschaltet. Das Gebäude selbst verfügt über kein elektronisches Schließsystem. Berlin: ☐ Ja ☑ Nein Stuttgart: ☐ Ja ☑ Nein Frankfurt: ☐ Ja ☑ Nein Hamburg: ☑ Ja ☐ Nein Der Eingang zum Büro sowie der Fluchtausgang verfügen über ein elektronisches Schließsystem. Meerbusch: ☐ Ja ☑ Nein Utrecht: ☑ Ja ☐ Nein Die Büro-Etage sowie der Fahrstuhl zum Büro können nur mithilfe der elektronischen Zutrittstechnik betreten werden. Cham: ☑ Ja ☐ Nein Die Eingangstüren und der Zugang zu den Büroräumen im 1. OG. Wien: ☐ Ja ☑ Nein Zürich: ☑ Ja ☐ Nein Der Gebäude-Haupteingang kann morgens bis 08.00 Uhr und abends ab 19.00 Uhr nur mithilfe der elektronischen Zutrittstechnik betreten werden. Untertags ist der Gebäude-Haupteingang offen. Der Eingang für das 1. OG kann auch mithilfe der elektronischen Zutrittstechnik betreten werden. Die Büros können nur mithilfe der elektronischen Zutrittstechnik betreten werden. Timisoara: ☑ Ja ☐ Nein Der Eingang zum Bürogebäude sowie alle Eingänge der einzelnen Stockwerke verfügen über elektronische Schließsysteme.
I.1.1.6	*Es werden folgende **Zutrittstechniken** angewandt:* München: ☑ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges Berlin: ☐ RFID ☐ PIN ☐ Biometrie ☑ Sonstiges: Mechanische Schlüssel. Für den Zugang zum Büro müssen zwei Türen mit unterschiedlichen Schlüsseln aufgeschlossen werden. Stuttgart: ☐ RFID ☑ PIN ☐ Biometrie ☐ Sonstiges Frankfurt: ☐ RFID ☐ PIN ☐ Biometrie ☑ Sonstiges: Mechanische Schlüssel Hamburg: ☑ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges Meerbusch: ☐ RFID ☐ PIN ☐ Biometrie ☑ Sonstiges: Mechanische Schlüssel Utrecht: ☑ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges Cham: ☑ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges

	Wien: ☐ RFID ☐ PIN ☐ Biometrie ☑ Sonstiges: Mechanische Schlüssel (für den Zugang zum Büro müssen zwei Türen mit dem gleichen Schlüssel geöffnet werden). Zürich: ☑ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges Timisoara: ☑ RFID ☐ PIN ☐ Biometrie ☑ Sonstiges: Mechanische Schlüssel für das Gebäude und den Fluchtausgang.
I.1.1.7	*Die Zutrittstechniken werden **personenspezifisch** vergeben:* Alle Standorte: ☑ Ja ☐ Nein
I.1.1.8	*Es existiert ein **mechanisches Schließsystem** für das Gebäude / die Büroräume:* Alle Standorte: ☑ Ja ☐ Nein Zürich: Für das Gebäude existiert ein mechanisches Schließsystem für den Seiteneingang. Für den Eingang in das 1. OG sowie für die Büroräume existieren neben den elektronischen Schließsystemen keine mechanischen Schließsysteme.
I.1.1.9	*Die **Ausgabe von Schlüsseln wird protokolliert**:* Alle Standorte: Ja, mittels eines Schlüsselbuchs.
I.1.1.10	*Die Schlüssel werden von folgenden **Abteilungen** ausgegeben:* München: Facility Management Berlin, Stuttgart, Frankfurt, Hamburg, Meerbusch, Utrecht: Standortverantwortlicher Cham: Standortverantwortlicher Wien: Standortverantwortlicher, Teamassistenz Zürich: Bürobetreiber (Das Züricher Büro befindet sich in einem Office-Center, in dem mehrere Unternehmen ihre Büros haben.) Timisoara: Office Management
I.1.1.11	*Der Zutritt für **betriebsfremde Personen** (etwa Besucherinnen und Besucher) zu den Büroräumen ist wie folgt beschränkt:* München: ☑ Ja ☐ Nein. Betriebsfremde Personen (einschließlich betriebsfremde Teilnehmer von Schulungen) werden am Eingang vom entsprechenden Ansprechpartner oder von Mitarbeitern der Rezeption abgeholt und sind nur in Begleitung befugt, sich im Gebäude zu bewegen. Berlin: ☑ Ja ☐ Nein. Betriebsfremde Personen klingeln an der Zugangstür. Nach erstem Gesprächskontakt über die Fernsprechanlage wird die Tür durch einen zuständigen Mitarbeiter geöffnet. Der Aufenthalt im Büro erfolgt nur in Begleitung eines Mitarbeiters. Stuttgart: ☑ Ja ☐ Nein. Es besteht eine Klingel mit Kamera- und Gegensprechmodul. Betriebsfremden Personen wird der Zugang nur nach Öffnung durch den zuständigen Mitarbeiter gewährt. Frankfurt: ☑ Ja ☐ Nein. Betriebsfremde Personen müssen an der Zugangstür klingeln. Diese wird von einem ATOSS-Mitarbeiter geöffnet. Vom Facility Management des Gebäudes beauftragte Handwerker erhalten für die Ausführung ihrer Arbeiten unmittelbaren Zugang. Hamburg: ☑ Ja ☐ Nein. Betriebsfremde Personen (einschließlich betriebsfremde Teilnehmer von Schulungen) werden am Eingang vom entsprechenden Ansprechpartner oder von Mitarbeitern der Rezeption abgeholt und sind nur in deren Begleitung befugt,

	sich im Gebäude zu bewegen. Beauftragte Firmen zur Büroreinigung und Wartung der EMA erhalten für die Ausführung ihrer Arbeiten unmittelbaren Zugang. Meerbusch: ☑ Ja ☐ Nein. Betriebsfremde Personen dürfen sich nur in Begleitung eines zuständigen Mitarbeiters auf den Büro-Etagen bewegen. Mittels Telefonsprechanlage wird die Identität geklärt, anschließend wird die Person von der Assistenz empfangen. Utrecht: ☑ Ja ☐ Nein. Betriebsfremde Personen dürfen sich nur in Begleitung eines zuständigen Mitarbeiters auf der Büro-Etage bewegen. Cham: ☑ Ja ☐ Nein. Betriebsfremde Personen klingeln an der Eingangstür. Nach erstem Gesprächskontakt über die Fernsprechanlage wird die Tür durch einen zuständigen Mitarbeiter geöffnet. Der Zugang zu den Büroräumen und der Aufenthalt im Büro erfolgt nur in deren Begleitung. Wien: ☑ Ja ☐ Nein. Betriebsfremde Personen (einschließlich betriebsfremder Teilnehmer von Schulungen) werden am Eingang vom entsprechenden Ansprechpartner oder der Teamassistenz abgeholt und sind nur in deren Begleitung befugt, sich im Gebäude zu bewegen. Zürich: ☑ Ja ☐ Nein. Betriebsfremde Personen dürfen sich nur in Begleitung eines Mitarbeiters in den Büroräumen aufhalten. Timisoara: ☑ Ja ☐ Nein. Betriebsfremde Personen werden am Eingang vom entsprechenden Ansprechpartner oder vom Office-Management abgeholt und sind nur in deren Begleitung befugt, sich im Gebäude zu bewegen.
I.1.2	**Rechenzentrum**
I.1.2.0	*Hinweis:* *Die Beschreibungen der folgenden Ziff. I.1.2.1 bis I.1.2.17 betreffen die hinsichtlich des Rechenzentrums am Sitz des Unternehmens in **München** (Rosenheimer Str. 141 h, 81671 München) getroffenen technischen und organisatorischen Maßnahmen. Alle Geschäftsstellen sowie alle Konzerngesellschaften der ATOSS Software AG (s. I.1.1.0) nutzen die gesamte IT-Infrastruktur des Unternehmenssitzes in München.*
I.1.2.1	*Die **Adresse** des Standorts des Rechenzentrums lautet:* Rosenheimer Str. 141 h, 81671 München
I.1.2.2	*Die in Ziff. I.1.1.0 genannten weiteren Geschäftsstellen und Konzerngesellschaften (i.S.v. §§ 15 ff. AktG) der ATOSS Software AG sind wie folgt an das Server-Netzwerk **angebunden**:* Alle Geschäftsstellen und Konzerngesellschaften, die auf Dienste des Rechenzentrums zugreifen und die über mehr als zehn Mitarbeiter verfügen, sind mittels verschlüsselter Standleitung mit der Zentrale verbunden und besitzen ausschließlich einen Domänen-Controller (DCs), um das lokale SUB-Netzwerk mit dem zentralen Netzwerk zu verbinden. Diese DCs sind in einem separaten abgeschlossenen Raum mit Klimatisierung und Alarmsicherung untergebracht und somit nicht ohne weiteres zugänglich. Bei Bedarf kann zu jeder Zeit die Verbindung zu einer Geschäftsstelle oder Konzerngesellschaft komplett abgeschaltet werden. Die systemkritischen IT-Einrichtungen befinden sich ausschließlich am Unternehmenssitz in München und werden von dort aus gesteuert und koordiniert.

I.1.2.3	*Das **Rechenzentrum** wird von folgender Einrichtung **betrieben**:* ☑ Auftragnehmer ☐ Dienstleister
I.1.2.4	*Die Auftragsdaten des Auftraggebers werden auf Servern des Auftragnehmers **physisch gespeichert**:* ☑ Ja ☐ Nein
I.1.2.5	*Die Auftragsdaten sind beim Auftragnehmer auf **mehr als ein Rechenzentrum** verteilt:* ☐ Ja ☑ Nein
I.1.2.6	*Das Rechenzentrum, auf dem die Auftragsdaten gespeichert werden, steht in folgender **Etage**:* ☐ EG ☑ Keller ☐ 1. OG Der Serverraum mit den Racks sowie Servern und Geräten befindet sich in einem eigenen Brandabschnitt im ersten Untergeschoss. Er ist fensterlos, umgrenzt von Massivwänden und hat einen doppelten Boden.
I.1.2.7	*Das Rechenzentrum verfügt über ein **elektronisches Schließsystem**:* ☑ Ja ☐ Nein
I.1.2.8	*Es wird folgende **Zutrittstechnik** verwendet:* ☑ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges
I.1.2.9	*Das Rechenzentrum ist mit einer **EMA** ausgestattet:* ☑ Ja ☐ Nein Der Zugangsbereich zum Rechenzentrum wird durchgängig von Kameras überwacht und durch das Personal des Auftragnehmers kontrolliert. Bei Alarm wird ein akustisches und optisches Signal ausgelöst und die Sicherheitsnotbeleuchtung eingeschaltet. Das Rechenzentrum ist in diesem Fall sofort zu verlassen.
I.1.2.10	*Die Zutrittstechniken sind **personenspezifisch** vergeben:* ☑ Ja ☐ Nein
I.1.2.11	*Die **Zutritte** (auch durch betriebsfremde Personen) auf das Rechenzentrum werden **protokolliert**:* ☑ Ja, sowohl erfolgreiche, als auch erfolglose Zutrittsversuche ☐ Ja, aber nur erfolgreiche Zutrittsversuche ☐ Nein
I.1.2.12	*Dabei werden die **Zutrittsdaten** ca. für folgenden Zeitraum **gespeichert**:* *Ca. 120 Tage.*
I.1.2.13	*Das Rechenzentrum verfügt über ein **mechanisches Schloss**:* ☑ Ja ☐ Nein
I.1.2.14	*Die Details zu Anzahl und Aufbewahrung der **Schlüssel** zum Rechenzentrum sind wie folgt festgelegt:*

	Anzahl Schlüssel: 10 Aufbewahrungsort: aus Sicherheitsgründen erfolgt keine Angabe
I.1.2.15	*Es haben folgende Personen mit folgenden Funktionen im Unternehmen des Auftragnehmers **Zutritt** zum Rechenzentrum:* Anzahl Personen: 10 Funktionen: IT, Facility Management, Notfallmanagement (Sicherheitsdienst)
I.1.2.16	*Der Zutritt durch **betriebsfremde Personen** zum Rechenzentrum ist wie folgt geregelt:* ☐ Keine Regelung ☑ Zutritt und Anwesenheit nur in Begleitung und mit Tagesakkreditierung Der Zutritt ist nur für im Voraus schriftlich benannte Personen möglich, d.h. eine schriftliche Anmeldung vor dem Besuch ist zwingend erforderlich. Die Benennung dieser Person ist allein dem „Access Authorizer“ erlaubt. Des Weiteren ist der Zugang zum Rechenzentrum nur dann erlaubt, wenn sich die betreffende Person mit einem Bildausweis (amtlicher Personalausweis, Reisepass oder Führerschein) identifiziert hat. Der Bildausweis muss während des Besuches im Rechenzentrum abgegeben werden und wird nach Beendigung der Arbeiten wieder ausgehändigt. Zugangsberechtigt ist nur, wer im Voraus die allgemeinen Verhaltensregeln sowie die Zugangsregelungen und Datenschutzbestimmungen gelesen und unterzeichnet hat. Mit der Unterschrift werden die Bestimmungen akzeptiert.
I.1.2.17	*Das Rechenzentrum wird für **weitere Zwecke** genutzt:* ☐ Ja ☑ Nein
I.2	**Zugriffskontrolle**
I.2.0	*Es besteht folgendes differenzierendes **Berechtigungskonzept**, das den Zugriff der Mitarbeiter auf die Daten des Auftraggebers regelt:* ☑ Ja ☐ Nein Es besteht ein Berechtigungskonzept, nach dem nur diejenigen Mitarbeiter Zugriff auf Auftragsdaten erhalten, für deren Arbeit der Zugriff unbedingt notwendig ist (Need-to-know-Prinzip, Erforderlichkeitsprinzip) und die formal berechtigt, fachlich befähigt und zuverlässig sind.
I.2.1	*Die Zugriffsberechtigungen werden wie folgt **vergeben**:* Zugriffe, Berechtigungen und Rechte werden durch ein zentrales Microsoft-„Active Directory“ bzw. eine firmeneigene Domäne definiert, koordiniert und kontrolliert. Jeder Mitarbeiter, der Zugriff auf die im Rechenzentrum gespeicherten hat, gehört grundsätzlich zu einer bestimmten Abteilung und erbt durch diese Zugehörigkeit allgemeine Zugriffsrechte und Berechtigungen. Spezielle Zugriffe und Berechtigungen, die vom Standard abweichen, werden auf Antrag (schriftlich oder per Email) an die IT-Abteilung gemeldet und nach Prüfung erteilt. Der Antrag muss außerdem durch den jeweiligen Vorgesetzten genehmigt sein. Änderungen in der Domäne, bei Berechtigungen und bei der Vergabe von Rechten werden zu Kontrollzwecken protokolliert und fristgerecht aufbewahrt.
I.2.2	*Mittels folgender Maßnahmen wird sichergestellt, dass **Unbefugte keinen Zugriff** auf die Auftragsdaten des Auftraggebers erhalten:*

	Der Auftragnehmer stellt sicher, dass personenbezogene Daten nur einem sehr begrenzten Mitarbeiterkreis zugänglich sind. Dieser Mitarbeiterkreis besteht aus den direkt am Projekt beteiligten Auftragnehmer-Beratern und -Entwicklern sowie den Mitarbeitern des Customer Service Centers (Hotline) des Auftragnehmers. Werden personenbezogene Daten zur Dokumentation im Trouble-Ticket-System des Auftragnehmers gespeichert, ist durch eine Berechtigungsvergabe sichergestellt, dass Unbefugte diese Daten nicht einsehen können.
I.2.3	*Hinsichtlich der Zugriffsberechtigungen im Falle eines **Abteilungs- / Funktionswechsels** oder des **Ausscheidens** eines Mitarbeiters sind folgende Maßnahmen getroffen:* Personelle Veränderungen werden der IT-Abteilung durch die Personalabteilung gemeldet. Die Berechtigungen werden je nach Art der Änderungen entzogen bzw. mittels zentralem Microsoft-„Active Directory“ bzw. mittels firmeneigener Domäne entsprechend angepasst.
I.2.4	*Die **Vergabe** und **Änderungen** von Zugriffsberechtigungen werden **protokolliert**:* ☑ Ja ☐ Nein
I.2.5	*Die vergebenen Rechte lassen sich zu Kontrollzwecken in Form von **Listen** exportieren:* ☑ Ja ☐ Nein
I.2.6	*Für den Fall der **Wartung** der Systeme gibt es getrennte Produktiv- und Testsysteme:* ☑ Ja ☐ Nein
I.2.7	*Es ist gewährleistet, dass der Datenaustausch **verschlüsselt** erfolgt:* ☑ Ja ☐ Nein Alle Endgeräte sind durch BIOS-Passwörter und Festplattenverschlüsselung entsprechend dem aktuellen Stand der Technik geschützt. Auf Laptops ist die Festplatte hardwareseitig durch das integrierte Verschlüsselungssystem des Herstellers mit AES265 verschlüsselt. Auf Smartphones und Tablets kommt ein Mobile Device Management (MDM) zum Einsatz, das die firmenbezogenen Daten in einem verschlüsselten Container vom Rest des Gerätes trennt. Der Datenaustausch zwischen den Geschäftsstellen erfolgt grundsätzlich über verschlüsselte VPN-Tunnel (IPSec). Ebenso erfolgen die VPN-Einwahlen von Mitarbeitern über IPSec-gesicherte Verbindungen. Für den Datenaustausch mit firmenfremden Geräten kommen hardware-verschlüsselte USB-Sticks (Iron keys) zum Einsatz, welche zusätzlich über einen integrierten Virenscanner verfügen.
I.2.8	*Die Systeme, auf denen die Daten des Auftraggebers im Rechenzentrum verarbeitet werden, sind über eine **Firewall** geschützt:* ☑ Ja ☐ Nein
I.2.9	*Die Firewall wird von folgender Einrichtung **administriert**:* ☑ Eigene IT ☐ Externer Dienstleister
I.2.10	*Der Zugang zum Firmennetzwerk durch **externe IT-Systeme** wird ausschließlich über **gesonderte Zugangspunkte** gewährt:* ☑ Ja ☐ Nein

	Für externe IT-Systeme stellt die IT-Abteilung separate Access Points zur Verfügung. Auf das externe IT-System haben ausschließlich diejenigen vom Auftragnehmer autorisierten Personen(gruppen) Zugriff, welche die geschützte, sichere Verbindung ins Netzwerk hergestellt haben.
I.3	**Datenträgerkontrolle / Speicherkontrolle**
I.3.0	*Nicht mehr benötigte elektronische **Datenträger** (Festplatten, CD-ROMs, DVDs, USB-Sticks), auf denen Auftragsdaten gesichert sind, werden wie folgt **entsorgt**:* Elektronische Datenträger werden durch einen externen Entsorgungsdienstleister physisch vernichtet. Die Löschung und Vernichtung erfolgt in Übereinstimmung mit internen Aufbewahrungsrichtlinien, gesetzlichen Aufbewahrungspflichten und anderen einschlägigen gesetzlichen Bestimmungen und betriebsinternen Regelungen. Vor jeder Vernichtung und Löschung von Datenträgern wenden sich Mitarbeiter stets an die IT-Abteilung des Auftragnehmers.
I.3.1	*Nicht mehr benötigte **Unterlagen** mit personenbezogenen Daten des Auftraggebers (Akten, Schriftwechsel etc.) im Unternehmen werden wie folgt **entsorgt**:* Die Vernichtung erfolgt durch einen Entsorgungsdienstleister. Hierzu sind in allen Geschäftsstellen und Konzernunternehmen verschlossene „Datentonnen“ aufgestellt, die regelmäßig sowie ggf. zusätzlich bei Erforderlichkeit geleert werden.
I.3.2	*Mit dem externen Entsorgungsdienstleister ist ein den gesetzlichen Vorgaben entsprechender **Vertrag zur Auftragsdatenverarbeitung** geschlossen:* ☑ Ja ☐ Nein
II.	**Integrität**
II.1	**Benutzerkontrolle**
II.1.0	*Es existiert eine Beschränkung des Zugangs zu den Datenverarbeitungsanlagen mittels Eingabe eines **Benutzernamens** und eines **Passwortes**:* ☑ Ja ☐ Nein
II.1.1	*Das IT-System verfügt – über den User-Account des Admins hinaus – über einen* **eigenständigen Admin-Account***:* ☑ Ja ☐ Nein
II.1.2	*Administrationsrechte werden **getrennt** von „normalen“ Nutzerrechten vergeben:* ☑ Ja ☐ Nein
II.1.3	*Es wird sichergestellt, dass die **Systemadministratorenkennung** für Nichtberechtigte unzugänglich ist und sicher verwaltet wird:* ☑ Ja ☐ Nein Grundsätzlich liegt die Verantwortlichkeit für die vollen Administrationsprivilegien (Zuweisung von Passwörtern und Änderungsregelungen) und für die Zugangskontrolle beim Leiter der IT-Abteilung. In Notfällen kann die jeweilige, nicht personifizierte **Domänen-Administratorenkennung** von einem definierten Personenkreis der IT-Abteilung verwendet werden. Diese wird unter Verschluss von der IT-Abteilung des Auftragnehmers verwaltet und in regelmäßigen Abständen geändert.

II.1.4	*Es ist sichergestellt, dass Nutzer nur auf Informationen **schreibend zugreifen** können, wenn dies für die Erfüllung ihrer Aufgaben im Unternehmen notwendig ist:* ☑ Ja ☐ Nein
II.1.5	*Passwörter werden mit einem dem Stand der Technik entsprechenden **Algorithmus** gehasht gespeichert:* ☑ Ja ☐ Nein
II.1.6	***Mobile Endgeräte** (Laptops, Smartphones, Tablets) verfügen über ein sicheres Authentifizierungsverfahren:* ☑ Ja ☐ Nein Zugriff auf mobile Endgeräte ist ausschließlich nach Authentifizierung über ein Passwortverfahren möglich
II.1.7	*Auf den Rechnern der Nutzer ist eine automatische passwortgeschützte **Bildschirmsperre** eingerichtet:* ☑ Ja ☐ Nein
II.1.8	*Hierbei wird der Bildschirm nach folgender **Zeit der Inaktivität** gesperrt:* Nach 10 Minuten.
II.1.9	*Es bestehen verbindliche Vorgaben zum **manuellen Sperren** des Rechners beim Verlassen des Arbeitsplatzes:* ☑ Ja ☐ Nein
II.1.10	*Nach **Verlust, Vergessen oder Ausspähen eines Passworts** werden folgende Maßnahmen ergriffen:* Der Administrator erstellt ein neues Passwort mit erzwungener Änderung durch den Mitarbeiter nach Erstanmeldung.
II.1.11	*Nach Erreichens der Höchstanzahl erfolgloser Anmeldeversuche werden die Zugänge wie folgt **gesperrt**:* Abhängig vom konkreten System
II.1.15	
II.1.16	
II.2	**Eingabekontrolle**
II.2.0	*Das **An- und Abmelden** von Nutzern in den IT-Systemen wird **protokolliert**:* Abhängig vom System
II.2.1	*Die Protokolldaten werden **zentral gespeichert und aufbewahrt**:* Abhängig vom System

	Diese werden nach den gesetzlichen Bestimmungen gespeichert und aufbewahrt.
II.2.2	*Die **Uhren** aller IT-Systeme sind **synchronisiert**, um die Auswertung von Logeinträgen zu ermöglichen:* ☑ Ja ☐ Nein
II.2.3	***Zugriffe** (in Form des Änderns oder des Löschens) auf die Auftragsdaten in den Software-Lösungen des Auftraggebers können personenbezogen **dokumentiert** werden:* Ändern ☑ Ja ☐ Nein Löschen ☑ Ja ☐ Nein Die Zugriffe des Auftragnehmers auf dem System des Auftraggebers können durch Verwendung der mit den Software-Lösungen des Auftragnehmers bereitgestellten Protokollierungsfunktionen protokolliert werden. Werden personenbezogene Daten zur Dokumentation im Trouble-Ticket-System des Auftragnehmers gespeichert, ist durch eine Protokollierungsfunktion feststellbar, welcher Benutzer wann welche Art und welchen Inhalt einer Änderung bzw. einer Löschung vorgenommen hat.
II.2.4	*Die Protokolle werden nach den gesetzlichen Vorgaben **aufbewahrt** und anschließend datenschutzkonform **gelöscht**:* ☑ Ja ☐ Nein
II.2.5	*Das (unbeabsichtigte) **Überschreiben** von personenbezogenen Daten wird wie folgt **vermieden**:* ☑ Ja ☐ Nein Durch die gezielte Vergabe von Berechtigungen für dezidierte Systeme wird der verändernde oder löschende Zugriff auf Auftragsdaten nur einem begrenzten Personenkreis ermöglicht. Zusätzlich beugen regelmäßig erstellte Backups einem Überschreiben von Auftragsdaten vor (siehe auch Ziff. III.3).
II.3	**Transportkontrolle**
II.3.0	*Die **Datenübermittlung** zwischen dem Auftragsverarbeiter und dem Auftraggeber erfolgt wie folgt:* Die Datenübermittlung erfolgt in der Regel mit verschlüsselter HTTP-Verbindung (SSL/HTTPS), aber auch per E-Mail (Text und Anhänge, etwa PDF-/Excel-/Word-Dateien), per FTP-Server oder per Einsichtnahme am Monitor (Fernwartung). Es kommt stets branchenübliche Fernwartungs-Software zum Einsatz, die verschlüsselt arbeitet und dem aktuellen Stand der Technik entspricht. Die Entscheidung, welche Fernwartungs-Software genutzt wird (z.B. Team Viewer, Cisco oder WebEx), obliegt dem Auftraggeber.
II.3.1	*Im Fall der elektronischen Datenübermittlung erfolgt ein **verschlüsselter** Transfer:* ☑ Ja ☐ Nein Abhängig vom verwendeten Kanal, verschlüsselte Kanäle sind in allen Fällen bevorzugt
II.3.3	
II.3.2	*Auftragsdaten des Auftraggebers werden auch auf **mobilen Endgeräten** (Laptops, Smartphones, Tablets) verarbeitet:* ☑ Ja ☐ Nein

II.3.3	***Anwender** werden über die Nutzung mobiler Endgeräte umfassend **informiert**:* ☑ Ja ☐ Nein Alle Mitarbeiter des Auftragnehmers werden über spezifische Risiken mobiler IT-Systeme (z.B. Ausspähen bei Nutzung in der Öffentlichkeit, Verlust oder Diebstahl) informiert und zur Ergreifung entsprechender Gegenmaßnahmen verpflichtet. Es ist ihnen untersagt, mobile Endgeräte an unberechtigte Dritte weiterzugeben.
II.3.4	*Mitarbeiter sind berechtigt, Auftragsdaten des Auftraggebers auf privaten (mobilen) Geräten zu verarbeiten (**Bring your own device**):* ☑ Ja ☐ Nein
II.3.5	*Mitarbeiter sind berechtigt, auf Daten des Auftraggebers von ihrem **Home Office** aus zuzugreifen:* Ja, die Entscheidung über eine Genehmigung liegt beim jeweiligen Auftraggeber.
II.4	**Übertragungskontrolle**
II.4.0	*Die Vorgänge der Datenübermittlung werden **dokumentiert**:* ☑ Ja ☐ Nein Wird im Rahmen der Fernwartung durch einen Auftraggeber der komplette Bestand der in der Software-Lösung des Auftragnehmers enthaltenen Daten an den Auftragnehmer übermittelt, werden Protokolle über die Verarbeitung dieses Datenbestands auf Systemen des Auftragnehmers geführt. Auf diese Weise bleibt nachvollziehbar, wann welcher Empfänger welche Daten erhält (etwa mithilfe der Zeitstempelung von E-Mails).
II.5	**Datenintegrität**
II.5.0	*Es sind technische Maßnahmen implementiert, die es ermöglichen, dass personenbezogene **Daten** auch bei einer Fehlfunktion des Systems **nicht beschädigt** werden:* ☑ Ja ☐ Nein Um die Datenintegrität zu gewährleisten, kommen neben Zutritts- und Zugriffskontrollen sowie Backup- und Restore-Strategien auch redundante Speichersysteme und eine automatische Spiegelung auf Backup-Systeme zum Einsatz.
II.6	**Trennbarkeit**
II.6.0	Es ist sichergestellt, dass die personenbezogenen Daten **ausschließlich für die festgelegten Zwecke verarbeitet** werden: ☑ Ja ☐ Nein Die Mitarbeiter des Auftragnehmers sind schriftlich auf die Einhaltung des Datengeheimnisses verpflichtet (§ 53 BDSG n.F.). Durch eine klare Aufgabentrennung und mittels betriebsinterner Datenschutzschulungen wird sichergestellt, dass die Mitarbeiter mit den Bestimmungen des Datenschutzrechts vertraut sind.
II.6.1	*Es ist gewährleistet, dass Auftragsdaten des Auftraggebers von anderen Daten **getrennt** werden:*

	Ja, durch logische Trennung.
II.6.2	*Es werden **unterschiedliche physische und virtuelle Systeme** mit eigenständigen Betriebssystemen und Datenbanken genutzt, für deren Nutzung die Anwender nur Rechte für jeweils ein System oder eine Datenbank erhalten:* ☑ Ja ☐ Nein
II.6.3	*Die zur Auftragsdatenverarbeitung eingesetzten Systeme sind **mandantenfähig**:* ☑ Ja ☐ Nein
II.6.4	*Es wird **Sandboxing** angewandt:* ☑ Ja ☐ Nein Der Auftragnehmer testet in isolierten Umgebungen neue Software und Geräte, ohne dass die Tests Auswirkungen auf die produktive Umgebung haben. Dies geschieht in dafür vorgesehenen isolierten virtuellen Umgebungen.
III.	**Verfügbarkeit und Belastbarkeit**
III.1	**Verfügbarkeitskontrolle**
III.1.1	Technische Maßnahmen
III.1.1.0	*Die IT-Systeme sind mit folgenden Mechanismen technisch vor **Datenverlusten** und **unbefugten Datenzugriffen** geschützt:* ☑ Virenschutz ☑ Anti-Spyware ☑ Spamfilter ☑ Firewall Alle Mechanismen sind auf dem aktuellen Stand der Technik. Die IT-Systeme des Auftragnehmers sind durch Hardwaremaßnahmen (Redundanzen), Softwarelösungen zum Schutz vor Malware/Spyware sowie durch Contentfilter für E-Mail und Web geschützt. Zudem wird das vorhandene Backup-Konzept zeitnah an geänderte Anforderungen (neue/entfernte Systeme) angepasst und die Wirksamkeit durch regelmäßige Wiederherstellungstests überprüft. Darüber hinaus ist eine zentrale Firewall mit IPS und Malware-Scanner im Einsatz, die sämtlichen Datenverkehr (einschließlich der Geschäftsstellen und Konzerngesellschaften) absichert. Dabei könnte etwa eine komplette Geschäftsstelle oder ein einzelnes System vom Datenaustausch ausgenommen werden.
III.1.2	Bauliche Maßnahmen
III.1.2.0	*Hinweis:* *Die Beschreibungen der folgenden Ziff. III.1.2.1 bis III.1.2.9 betreffen die hinsichtlich des Rechenzentrums am Unternehmenssitz in **München** (Rosenheimer Str. 141 h, 81671 München) getroffenen baulichen Maßnahmen. Alle Geschäftsstellen sowie alle Konzerngesellschaften (s. I.1.1.0) nutzen die gesamte IT-Infrastruktur der ATOSS Software AG in München.*

III.1.2.1	*Fest installierte **Datenleitungen** sind durch bauliche Maßnahmen vor **Beschädigung** geschützt:* ☑ Ja ☐ Nein Alle Datenleitungen, die nicht in den eigenen oder gemieteten Flächen des Gebäudes verlaufen, sind durchgängig sabotagesicher durch Panzerstahlrohre geschützt.
III.1.2.2	*Der Serverraum und der USV-Raum (Raum für die Gewährleistung der unterbrechungsfreien Stromversorgung) sind mittels einer **EMA** alarmgesichert:* ☑ Ja ☐ Nein (s. I.1.2.9)
III.1.2.3	*Die **Außenwände** des **Serverraumes** sowie des **USV-Raums** bestehen aus folgendem Material:* Aus massiver Brandschutzwand. Des Weiteren ist eine T90HS-Sicherheitstür installiert.
III.1.2.4	*Der Server-Raum und USV-Raum verfügen über **Fenster**:* ☐ Ja ☑ Nein
III.1.2.5	*Der Serverraum und der USV-Raum sind **klimatisiert**:* ☑ Ja ☐ Nein Sowohl die Klimatisierung als auch die Stromversorgung sind redundant aufgebaut.
III.1.2.6	*Es besteht ein automatisches **Löschsystem** im Serverraum und im USV-Raum:* ☐ Ja ☑ Nein Aber es stehen manuelle CO2-Löscher zur Verfügung.
III.1.2.7	*Der Serverraum und USV-Raum verfügen über **Rauchmelder**:* ☑ Ja ☐ Nein Zusätzlich besteht ein Rauchansaug- und Brandfrüherkennungssystem, welches über einen eigenen Rauchmelder verfügt.
III.1.2.8	*Es besteht ein Anschluss an eine **Brandmeldezentrale**:* ☑ Ja ☐ Nein
III.1.2.9	*Es besteht ein System verschiedener **Brandabschnitte**:* ☑ Ja ☐ Nein Die Räumlichkeiten der IT in der der ATOSS Software AG in München sind in mehrere Brandabschnitte unterteilt. Der Serverraum mit den Racks sowie Servern und Geräten befindet sich einem Brandabschnitt (1) im 1. Untergeschoss (UG1). Die redundanten USVen befinden sich in einem angrenzenden, aber getrennten Brandabschnitt (2), ebenfalls im UG1. Die redundanten Klimageräte befinden sich ebenfalls im UG1, aber in einem nicht an den Server- oder USV-Raum angrenzenden Brandabschnitt (3). Die Netzersatzanlage befindet sich auf dem Dach und somit ebenfalls in einem anderen Brandabschnitt (4). Die Büroräume befinden sich im 5. bis 9. OG des Gebäudes. Jedes Bürogeschoss hat einen eigenen Technikraum in jeweils einem getrennten Brandabschnitt.
III.2	**Zuverlässigkeit**

III.2.0	*Eine **unterbrechungsfreie Stromversorgung** im USV-Raum ist **gewährleistet**:* ☑ Ja ☐ Nein Die USV ist redundant. Die Funktionsfähigkeit der USV ist durch einen Service- und Wartungsvertrag mit dem Stromanbieter vertraglich abgesichert.
III.2.1	*Das Rechenzentrum sowie der USV-Raum verfügen darüber hinaus über eine **Netzersatzanlage** (Dieselaggregat):* ☑ Ja ☐ Nein
III.2.2	*Es ist sichergestellt, dass **kritische IT-Systeme** nur auf das absolut **notwendige Maß** beansprucht werden:* ☑ Ja ☐ Nein Auf kritischen IT-Systemen dürfen keine Entwicklungen oder Tests durchgeführt werden. Alle Netzwerkdienste, die nicht zur Aufgabenerfüllung benötigt werden, sind deinstalliert, abgeschaltet oder aufgrund geeigneter Filter unzugänglich. Jegliche Anwendungssoftware, die nicht zur Aufgabenerfüllung benötigt wird, ist deinstalliert. Sämtliche Zugriffsrechte auf kritische IT-Systeme sind auf ein Mindestmaß reduziert.
III.3	**Wiederherstellbarkeit**
III.3.0	*Beim Auftragsverarbeiter existiert ein dokumentiertes **Backup-Konzept**:* ☑ Ja ☐ Nein
III.3.1	*Es werden folgende **Sicherungsmedien** in Anspruch genommen:* Sicherungsbänder, Festplatten und ein redundantes Storage-System.
III.3.2	*Die Backups werden wie folgt **durchgeführt**:* Backups werden per Echtzeitspiegelung erstellt. Die Daten werden vollständig automatisiert und, über ein Storage-System gepuffert, auf Magnetband geschrieben. Es werden dem technischen Stand entsprechende und den Anforderungen angemessene, regelmäßig aktualisierte Firewall-Systeme und Antiviren-Systeme eingesetzt.
III.3.3	*Die Backups der Systeme werden in folgenden **Zeitabständen** erstellt:* Mehrfach täglich.
III.3.4	*Die Backups werden an folgenden **Orten** aufbewahrt:* Redundantes Storage-System im Rechenzentrum, feuerfester und dokumentensicherer Safe in getrenntem Brandabschnitt, Sicherheitsdienst an anderem Ort.
III.3.5	*Dabei werden Backups auch in einem vom Ort des primären Servers **getrennten** Brandabschnitt / Gebäudeteil aufbewahrt:* ☑ Ja ☐ Nein
III.3.6	*Es werden **wöchentliche** und **tägliche** Backups geographisch voneinander **getrennt** aufbewahrt:* ☑ Ja ☐ Nein
III.3.7	*Die Daten der Backups sind **verschlüsselt**:*

	☑ Ja ☐ Nein Die Verschlüsselungsmethoden entsprechen dem aktuellen Stand der Technik.
III.3.8	*Der **Transport** der Backups wird wie folgt durchgeführt:* Abholung durch einen Sicherheitsdienst.
III.3.9	*Das Backup-Konzept kann dem Auftraggeber auf Anfrage **vorgelegt** werden:* ☐ Ja ☑ Nein Das Backup-Konzept kann aus Sicherheitsgründen nicht vorgelegt werden.
III.3.10	*Im Unternehmen existiert ein dokumentiertes **Notfallkonzept** (im Fall von Hardwaredefekten / Brand / Totalverlust etc.):* ☑ Ja ☐ Nein Für verschiedene Eskalationsstufen von Datenverlust gibt es verschiedene Konzepte. Die Kernkomponenten der Infrastruktur (Hardware-Server) werden durch ein proaktiv agierendes Managementsystem überwacht, das bei Ausfall einer Komponente, teilweise schon bei drohendem Ausfall, automatisch eine entsprechende Meldung an den Hersteller absetzt. Dies gilt auch für die zentralen Storage-Systeme im Rahmen von Selbst-Überwachungsmaßnahmen. Auf diese Weise ist gewährleistet, dass entsprechende Komponenten proaktiv durch die jeweiligen Hersteller ersetzt oder repariert werden. Um im Falle eines Brandes oder eines anderen Totalverlustes den Geschäftsbetrieb schnellstmöglich wieder aufnehmen zu können, werden aktuelle Sicherungen zusätzlich außer Haus bei einem Sicherheitsdienst gelagert.
IV.	**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**
IV.1	**Überprüfung der Maßnahmen**
IV.1.0	*Es werden verfügbare **Sicherheitsupdates** für die System- und Anwendungssoftware nach einem implementierten Verfahren getestet, bei Eignung freigegeben und nach ihrer Freigabe umgehend installiert:* ☑ Ja ☐ Nein
IV.1.1	*Die **Firewall** wird regelmäßig auf Updates hin **überprüft** und werden diese auf die Systeme geladen:* ☑ Ja ☐ Nein
IV.1.2	*Die Funktionalität der unterbrechungsfreien Stromversorgung (**USV**) im Serverraum wird regelmäßig **überprüft**:* ☑ Ja ☐ Nein
IV.1.3	*Das System der Wiederherstellung durch ein **Backup** wird regelmäßig auf Funktionalität hin **überprüft**:* ☑ Ja ☐ Nein Die Wiederherstellung und Konsistenz von Backup-Dateien wird quartalsweise geprüft.
IV.1.4	Es werden **Penetrationstests** durchgeführt und dokumentiert: ☑ Ja ☐ Nein

	Einmal halbjährlich werden Penetrationstests (Restore-Tests, NEA, etc.) sowie Wartungen (NEA, BFE, Monitoring-System, etc.) durch den Auftragnehmer selbst oder durch Wartungspartner durchgeführt und dokumentiert.
IV.2	**Datenschutzfreundliche Voreinstellungen**
IV.2.0	*Die Software-Lösungen bieten die technische Möglichkeit,* ***Schnittstellen*** *zu* ***verhindern bzw. zu schließen****:* ☑ Ja ☐ Nein In einigen Software-Lösungen des Auftragnehmers können Schnittstellen zu anderen Systemen mithilfe verschiedener Parameter begrenzt werden. Insbesondere ist es möglich, die Benutzung einer Schnittstelle nur entsprechend berechtigten Personen zugänglich zu machen. Weiterhin können bestimmte Prozesse über Schnittstellen derart automatisiert werden, dass sie nur zu einer bestimmten Zeit ablaufen.
IV.2.1	Die **Qualitätssicherungsprozesse** in der Softwareentwicklung basieren auf etablierten und vereinbarten Standards: ☑ Ja ☐ Nein
IV.2.2	Die Datensicherheit der vom Auftragsverarbeiter hergestellten Software-Lösungen gegen unerlaubten Zugriff („**Backdoors**“) ist sichergestellt: ☑ Ja ☐ Nein
IV.2.3	*Die Software-Lösungen bieten die technische Möglichkeit, einzelne Funktionen zu* ***deaktivieren, ohne*** *dass das* ***Gesamtsystem in Mitleidenschaft gezogen*** *wird:* ☑ Ja ☐ Nein Einzelne Funktionen der Software-Lösungen des Auftragnehmers sind deaktivierbar, ohne dass sich die Deaktivierung auf die Funktionalität der Software-Lösungen im Übrigen auswirkt. Die Software-Lösungen bestehen aus unterschiedlichen Modulen, die nur teilweise aufeinander aufbauen und deren Funktionalität nur teilweise von der eines anderen Moduls abhängen.
IV.2.4	*Es besteht eine Möglichkeit zur Zusammenstellung, Berichtigung, Sperrung und Löschung aller personenbezogener Daten einer Person (Single Point of Contact (****SPoC****):* ☑ Ja ☐ Nein
IV.3	**Auftragskontrolle**
IV.3.0	*Es wird wie folgt sichergestellt, dass Mitarbeiter Auftragsdaten des Auftraggebers* ***nur im Auftrag*** *und entsprechend der Anweisungen des Auftraggebers verarbeiten:* Durch schriftliche Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 53 BDSG n.F.) sowie wiederkehrende Belehrungen im Rahmen regelmäßiger Schulungen zum Datenschutz.
IV.3.1	*Es wird wie folgt sichergestellt, dass auch* ***Unterauftragnehmer*** *des Auftragnehmers Auftragsdaten des Auftraggebers nur im Auftrag und entsprechend der Anweisungen des Auftraggebers verarbeiten:* Zwischen dem Auftragnehmer und seinen Unterauftragnehmern wurden Verträge über die Auftragsverarbeitung gemäß den Anforderungen nach Art. 28 DS-GVO bzw. § 62 Abs. 3 BDSG n.F. geschlossen. In den Verträgen ist insbesondere festgelegt, dass der

	Auftraggeber weisungsbefugt ist und die Mitarbeiter des Unterauftragnehmers auf das Datengeheimnis verpflichtet sind.
IV.3.2	*Alle Mitarbeiter, die Auftragsdaten verarbeiten, werden nachweislich im aktuell geltenden Datenschutzrecht **geschult**:* Ja, im Rahmen regelmäßiger Präsenz- und Online-Schulungen.
IV.3.3	*Bei der Konzerngesellschaft ATOSS Software AG (Deutschland) ist ein betrieblicher Datenschutzbeauftragter bestellt:* ☑ Ja ☐ Nein
IV.3.4	*Die **Kontaktdaten** des DSB der ATOSS Software AG (Deutschland) lauten wie folgt:* Dr. Maximilian Hoffmann 089 / 42771 – 125 maximilian.hoffmann@atoss.com
IV.3.5	*Der DSB verfügt nachweislich über folgende **Qualifikation**:* Teilnahme an anerkanntem Lehrgang zum Datenschutzbeauftragten.
IV.3.6	*Es können eine **Bestellungsurkunde** und ein **Fachkundenachweis** vorgelegt werden:* Kopien beider Nachweise sind vorhanden und können dem Auftraggeber auf Verlangen vorgelegt werden.
IV.3.7	*Der Auftragnehmer setzt zur Erfüllung der Pflichten aus dem Vertrag mit dem Auftraggeber weitere **Unterauftragnehmer** ein:* ☑ Ja ☐ Nein
IV.3.8	*Der **Auftraggeber** hat **Kenntnis** von den eingesetzten Unterauftragnehmern und diese sind vom Auftraggeber **genehmigt**:* ☑ Ja ☐ Nein Im Rahmen der Vereinbarung zur Auftragsverarbeitung.
IV.3.9	*Es sind folgende Maßnahmen implementiert, um zu gewährleisten, dass die **Unterauftragnehmer** die **Vorgaben** des Vertrags mit dem Auftraggeber und die Weisungen des Auftraggebers **umsetzen**:* Die Beschreibung der technischen und organisatorischen Maßnahmen der Unterauftragnehmer sind vom Auftragnehmer überprüft worden.

Hinweis: Im Falle von Änderungen der getroffenen und dokumentierten technischen und organisatorischen Maßnahmen (Anlage 1 zur Vereinbarung zur Auftragsverarbeitung) wird dem Auftraggeber die jeweils mit aktuellem Tagesdatum versehene Fassung der Anlage 1 auf geeignete Weise zur Verfügung gestellt, z.B. auf einem über die Website des Auftragnehmers zugänglichen Online-Portal. Der Auftraggeber ist verpflichtet, sich regelmäßig über die aktuelle Fassung der Anlage 1 zu informieren.

Anlage 2 – Genehmigte Unterauftragnehmer

	Unternehmen	Adresse	Tätigkeitsbeschreibung
	ATOSS Konzerngesellschaften		
1.	ATOSS Software AG	Rosenheimer Str. 141 h, 81671 München	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen
2.	ATOSS CSD Software GmbH	Rodinger Straße 19 93413 Cham	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen
3.	ATOSS Software Ges.m.b.H.	Ungargasse 64-66, Stiege 3, Top 503 1030 Wien, Österreich	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen
4.	ATOSS Software AG (Schweiz)	Badenerstrasse 549 8048 Zürich, Schweiz	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen
5.	SC ATOSS Software SRL	Bd. Liviu Rebreanu Nr. 76-78 300755 Timisoara, Rumänien	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen
	Andere Gesellschaften		
6.	Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Hosting, Datenspeicherung
7.	Host Europe GmbH	Welserstraße 14, 51149 Köln	Hosting, Datenspeicherung
8.	ODAV AG	Ernst-Heinkel-Straße 11, 94315 Straubing	Hosting, Datenspeicherung
9.	The Rocket Science Group LLC d/b/a Mailchimp	675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308, USA	Email-Newsletter sowie Emailbenachrichtigungen

Anlage 3 - Technische und organisatorische Maßnahmen der weiteren Unterauftragnehmer

In den Anhängen befinden sich als separate Dokumente:

- Technische und organsiatorische Maßnahmen der Hetzner Online GmbH
- Technische und organsiatorische Maßnahmen der Host Europe GmbH
- Technische und organisatorische Maßnahmen der ODAV AG

Die technischen und organisatorischen Maßnahmen der „The Rocket Science Group LLC“ finden sich hier: https://mailchimp.com/about/security/