Die ATOSS CSD Software GmbH (als Auftragsverarbeiter - nachstehend "**ATOSS**" genannt) und der Kunde (als datenschutzrechtlich Verantwortlicher - nachstehend "**Auftraggeber**" genannt) (nachstehend einzeln oder gemeinsam auch „**Parteien**" genannt) haben eine Leistungsvereinbarung über die Bereitstellung von Software-Produkten durch ATOSS und damit zusammenhängende technische Dienstleistungen geschlossen. Die nachfolgende Vereinbarung zur Datenverarbeitung im Auftrag dient als Grundlage zur Erfüllung der gesetzlichen Bestimmungen zum Datenschutz im Hinblick auf die bestehenden Vertragsverhältnisse der Parteien über die Erbringung von Dienstleistungen betreffend die dem Kunden von ATOSS zur Nutzung zur Verfügung gestellten Software-Lösungen (On-Premise-Lösung oder Cloud-Lösung) durch ATOSS.

Soweit ATOSS in diesem Zusammenhang personenbezogene Daten der Beschäftigten des Kunden (nachfolgend: Auftragsdaten) verarbeitet, gelten hierfür die Bedingungen der nachfolgenden Vereinbarung über die Datenverarbeitung im Auftrag.

Vereinbarung über die Datenverarbeitung im Auftrag

Inhaltsverzeichnis:

Anlagen:

Präambel

(1) Gesetzliche Grundlage

Die gesetzlichen Grundlagen bilden die Bestimmungen der EU-Datenschutzgrundverordnung (nachfolgend: DS-GVO) und des Bundesdatenschutzgesetzes in der jeweils geltenden Fassung (nachfolgend: BDSG). Soweit im Rahmen dieser Vereinbarung nicht ausdrücklich abweichend definiert, haben die verwendeten Begriffe, z.B. „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“ oder „Pseudonymisierung“ dieselbe Bedeutung wie in Art. 4 DS-GVO.

(2) 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 ATOSS, für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch ATOSS sowie für die Wahrung der Rechte der Betroffenen, allein verantwortlich.

§ 1 - Gegenstand und Dauer der Verarbeitung

(1) Gegenstand

ATOSS erbringt für den Auftraggeber Dienstleistungen betreffend die von ATOSS vertriebenen Softwareprodukte. Diese Dienstleistungen umfassen regelmäßig auch Sachverhalte der Auftragsverarbeitung, da ATOSS bei deren Durchführung verschiedentlich personenbezogene Daten des Auftraggebers im Auftrag, nach Weisung und im Interesse des Auftraggebers verarbeitet. Die Vereinbarung gilt entsprechend für (Fern-)Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann.

(2) Dauer

Die Laufzeit dieser Vereinbarung entspricht der Dauer der Zusammenarbeit der Parteien auf Basis der jeweiligen Leistungsvereinbarungen.

§ 2 - Auftragsinhalt im Einzelnen

(1) Art und Zweck der Verarbeitung

(a) Art

Auftraggeber und ATOSS stehen in einer geschäftlichen Beziehung, in deren Rahmen ATOSS Dienstleistungen für den Auftraggeber erbringt. Diese können nach Maßgabe der zugrundeliegenden Leistungsvereinbarung insbesondere folgende Arten der Verarbeitung umfassen:

- Customizing i.S.v. Parametrierung der von ATOSS als On-Premise-Lösung oder als Cloud-Lösung bereitgestellten Standard-Software (insbesondere Unterstützung beim Anlegen der Mitarbeiter-Stammsätze in der Datenbank der dem Auftraggeber von ATOSS zur Nutzung bereitgestellten Standard-Software, beim Einrichten von Arbeitszeitmodellen und Zeitkonten usw.) und Anpassung bzw. Scripting von Standard-Schnittstellen.
- Softwarepflege-Leistungen betreffend die von ATOSS als On-Premise-Lösung oder als Cloud-Lösung bereitgestellte Standard-Software (insbesondere Unterstützung bei Software-Release-Wechseln sowie bei der Behebung von vom Auftraggeber gemeldeten Fehlfunktionen).
- Hotline-Leistungen betreffend die von ATOSS als On-Premise-Lösung oder als Cloud-Lösung bereitgestellte Standard-Software (insbesondere 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 Erfassungs-Terminals).
- Prüfungs- und Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen zur Sicherstellung der Betriebsbereitschaft der im Rahmen der Cloud Solution bereitgestellten Standard-Software.
- Managed Service Leistungen betreffend die Administration von personenbezogenen Daten gemäß des im jeweiligen Einzelvertrag festgelegten Umfangs (insbesondere aktive Unterstützung bei der Administration von personenbezogenen Daten von Mitarbeitern des Auftraggebers in der von ATOSS bereitgestellten Standard-Software).

Ein Teil der Leistungserbringung kann dabei:

- vor Ort beim Auftraggeber (nach dessen Wahl durch Direktzugriff auf seine IT-Systeme oder durch Herstellung einer Verbindung zwischen einem Client-Rechner von ATOSS und den IT-Systemen des Auftraggebers),

- per Fernzugriff über eine vom Auftraggeber bereitgestellte geeignete Softwarelösung zum Fernzugriff (z.B. VPN, Desktop Sharing), die auf aktuellen Windows Server Betriebssystemen lauffähig ist (inkl. notwendiger Lizenz).

erfolgen.

In allen Fällen ist eine lesende und schreibende Zugriffsmöglichkeit durch ATOSS auf die in der Datenbank der Standard-Software befindlichen Auftragsdaten nicht auszuschließen.

(b) Zweck

Zweck der Verarbeitung ist die Gewährleistung der Funktionalität und ggf. der Aktualität der dem Auftraggeber von ATOSS zur Nutzung zur Verfügung gestellten Software-Lösung.

(2) Kategorien der personenbezogenen Daten

ATOSS verarbeitet im Rahmen dieses Vertragsverhältnisses in der Regel die folgenden Kategorien personenbezogener Daten des Auftraggebers. Welche Kategorien personenbezogener Daten im jeweiligen Vertragsverhältnis verarbeitet werden, hängt davon ab, welche Daten der Auftraggeber ATOSS konkret zur Verarbeitung überlässt.

Mitarbeiterstammdaten und zeitwirtschaftliche Informationen

- Stammdaten wie z.B.:
    - Personalnummer
    - Anrede, Name, Vorname
    - Geburtsdatum
    - Kartennummer(n) des / der Ausweis(e)
    - Mitarbeiterkategorie (z.B. Zuordnung zum Abrechnungsmodell)
    - Sonstige vertragsrelevante Daten wie Eintritts-, Austritts- Umgruppierungsdaten
    - Vereinbarungen zur Arbeitszeit sowie Beginn und Ende der zeitwirtschaftlichen Betrachtung
    - 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 Zeitsalden / Zeitkonten
- Informationen über einzelvertragliche, tarifliche und sonstige Vergütungs-, Urlaubs- und Freizeitansprüche von Mitarbeitern:
    - generelle Vereinbarungen
    - Werte und Salden
- Informationen über geplante und tatsächliche Abwesenheiten
- Informationen über Buchungen / Stempelungen inkl. Uhrzeit und Ort der Buchung / Stempelung
- Informationen über tatsächliche Anwesenheits-, (Ruf-)Bereitschafts- und Arbeitszeiten
- Informationen über Zugehörigkeit zu Organisationseinheiten, Projekten, Aufträgen, Kostenstellen, Arbeitsplätzen etc. und den dafür geleisteten Zeiten
- Kantinenbuchungen
- Manuelle Anmerkungen zu Stamm- und Bewegungsdaten
- Systemseitige Warnungen und Fehlermeldungen bei Abweichungen von Vorgaben oder Regeln

Informationen aus der Personaleinsatzplanung

- 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

Antragswesen und Aufgabenmanagement

- 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

Informationen des Zutrittsmanagements

- Informationen über Zutrittsberechtigungen für bestimmte Geräte, Zonen und Zeiträume
- Zugangskennungen
- PIN für Eingabe am Gerät
- Identifikationsmerkmale für biometrische Zutrittssicherung (Fingerprint-Verfahren etc.)
- Informationen über tatsächlichen oder versuchten Zutritt bzw. Verlassen von Zonen inkl. Uhrzeit und Ort der Buchung

Systembezogene Informationen

- 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. § 26 Abs. 8 BDSG

(4) Sachliche und örtliche Beschränkung der Verarbeitung

(a) Sachlich

Eine über diese Vereinbarung hinausgehende Verarbeitung von Auftragsdaten ist ATOSS nicht gestattet. Eine Verarbeitung für andere Zwecke, insbesondere die eigenmächtige Weitergabe von Auftragsdaten an Dritte, ist nicht zulässig. ATOSS ist verpflichtet, die Auftragsdaten verschiedener Kunden getrennt zu verarbeiten.

(b) Örtlich

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union (nachfolgend: EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (nachfolgend: EWR) statt.

ATOSS wird die vertraglich vereinbarte Leistung ggf. von den in Anlage 2 vereinbarten Leistungsstandorten aus durch die genehmigten Unterauftragsverarbeiter (siehe § 6) erbringen.

Diese Unterauftragsverarbeiter sind teilweise nicht in einem Mitgliedsstaat der EU oder in einem anderen Vertragsstaat des EWR ansässig (nachfolgend: Drittstaat). Eine Datenübermittlung an einen Unterauftragsverarbeiter in einem Drittstaat erfolgt jedoch nur, wenn zuvor die besonderen Voraussetzungen der Art. 44 ff. DS-GVO (Grundsätze der Übermittlung personenbezogener Daten an Drittstaaten) erfüllt sind (vgl. § 6 Abs. (2) lit. b dieser Vereinbarung).

§ 3 - Technische und organisatorische Maßnahmen

(1) Gewährleistung der Datensicherheit

ATOSS hat die Grundsätze ordnungsgemäßer Datenverarbeitung zu beachten und ihre Einhaltung zu überwachen (vgl. Art. 5 DS-GVO). ATOSS versichert, dass ATOSS die Regelungen der Art. 28 Abs. 3 lit. c, 32 DS-GVO einhält. ATOSS 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. Zur Bestimmung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung, insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder der unbefugten Offenlegung von beziehungsweise dem unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden, verbunden sind. 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.

(2) Dokumentation und Vorlage der Maßnahmen

ATOSS hat die technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung mit Blick auf die konkrete Auftragsdurchführung zu dokumentieren und stellt dem Auftraggeber diese Dokumentation auf Anfrage zur Verfügung.

(3) Aktueller Stand der Technik und technische Anpassungen

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es ATOSS gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dieser Vereinbarung festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen sind zu dokumentieren und dem Auftraggeber auf geeignete Weise mitzuteilen, z.B. auf einem über die Website von ATOSS zugänglichen Online-Portal.

ATOSS stellt dem Auftraggeber in diesem Fall auf Anfrage eine aktualisierte Beschreibung dieser Maßnahmen zur Verfügung, die es dem Auftraggeber ermöglicht, die Einhaltung der Vorgaben des § 3 Abs. 1 dieser Vereinbarung zu prüfen. Durch diese Bereitstellung räumt ATOSS dem Auftraggeber die Möglichkeit ein, diesen Änderungen innerhalb von vier Wochen zu widersprechen. Der Auftraggeber ist nur dann zum Widerspruch berechtigt, wenn die Änderungen nicht den Anforderungen der § 3 Abs. 1 und § 3 Abs. 2 dieser Vereinbarung entsprechen. Widerspricht der Auftraggeber den Änderungen nicht innerhalb der Widerspruchsfrist, gilt die Zustimmung zu den Änderungen als erteilt. Im Falle eines Widerspruchs kann ATOSS den Teil der Dienstleistung aussetzen, der von dem Widerspruch des Auftraggebers betroffen ist.

§ 4 - Weisungsbefugnis

(1) Dokumentierte Weisung

Der Auftraggeber hat das Recht, ATOSS 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. ATOSS darf die Auftragsdaten nur nach dokumentierter Weisung des Auftraggebers verarbeiten, es sei denn, ATOSS 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

ATOSS hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung sei rechtswidrig. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. ATOSS 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 ATOSS nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an ATOSS wendet, wird ATOSS dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(5) Auftragsfremde Weisungen

Über die Ausführung von Weisungen des Auftraggebers, die über die in dieser Vereinbarung geregelten Leistungen hinausgehen, entscheidet ATOSS. ATOSS kann in diesem Fall eine gesonderte Vergütung beanspruchen.

(6) Regress

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

§ 5 - Verpflichtung zur Vertraulichkeit

(1) Daten- und Fernmeldegeheimnis

ATOSS und jede ATOSS unterstellte Person, die Zugang zu Auftragsdaten hat, sind zur Vertraulichkeit verpflichtet, insbesondere gemäß den Bestimmungen der Art. 5 Abs. 1 f), Art. 28 Abs. 3 b), Art. 29 und Art. 32 Abs. 4 DS-GVO sowie des § 88 TKG. Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung dieser Vereinbarung fort.

(2) Unterweisung aller zur Auftragsverarbeitung eingesetzten Personen

ATOSS 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 Unterauftragsverarbeitern

(1) Begriff des Unterauftragsverarbeiters

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 ATOSS 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. ATOSS 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

Die Beauftragung von Unterauftragsverarbeitern ist nur nach Zustimmung des Auftraggebers möglich.

(a) Allgemeine Anforderungen

Jeder Unterauftragsverarbeiter ist verpflichtet, sich vor Beginn der Verarbeitungstätigkeiten schriftlich dazu zu verpflichten, dieselben Datenschutzverpflichtungen einzuhalten, wie in dieser Vereinbarung vereinbart, sofern nicht ausdrücklich etwas anderes vereinbart wurde. Der Unterauftragsverarbeitungsvertrag muss zumindest das nach dieser Vereinbarung erforderliche Datenschutzniveau gewährleisten. Jeder Unterauftragsverarbeiter muss sich insbesondere dazu verpflichten, die vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen gemäß Art. 32 DS-GVO einzuhalten und ATOSS eine Liste der umgesetzten technischen und organisatorischen Maßnahmen zur Verfügung zu stellen, die dem Auftraggeber auf Verlangen zur Verfügung gestellt wird. Die Maßnahmen des Unterauftragsverarbeiters können von dem zwischen Auftraggeber und ATOSS Vereinbarten abweichen, dürfen jedoch nicht unter das Datenschutzniveau fallen, welches durch die Maßnahmen von ATOSS gewährleistet wird. Weigert sich ein Unterauftragsverarbeiter, sich denselben datenschutzrechtlichen Pflichten zu unterwerfen, wie sie in dieser Vereinbarung niedergelegt sind, kann der Auftraggeber dem zustimmen, wobei diese Zustimmung nicht unbilliger Weise verweigert werden darf.

(b) Unterauftragsverarbeiter in Drittstaaten

Für den Fall, dass ein Unterauftragsverarbeiter in keinem Drittstaat ansässig ist, welcher gemäß Art. 45 DS-GVO ein angemessenes Datenschutzniveau bietet, wird ATOSS diesem Umstand ausreichend Rechnung tragen. ATOSS wird mit diesem Unterauftragsverarbeiter einen Vertrag zur Datenverarbeitung im Auftrag abschließen, der zusätzlich zu den in (a) aufgeführten Regelungen auf den EU-Standardvertragsklauseln (Beschluss 2021/914 - Modul Drei – Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter) oder anderen Standarddatenschutzklauseln für Auftragsverarbeiter beruht, soweit diese nach Art. 46 Abs. 2 lit. c DS-GVO zugelassen sind. ATOSS ist auch zum Abschluss von Standardvertragsklauseln oder anderen Standarddatenschutzklauseln im Namen und zu Gunsten des Auftraggebers berechtigt. Der Auftraggeber ermächtigt ATOSS hiermit zum Abschluss einer solchen Vereinbarung im eigenen Namen.

(3) Gegenwärtige Unterauftragsverarbeiter

Hinsichtlich der mit ATOSS i.S.v. §§ 15 ff. AktG verbundenen Unternehmen sowie der sonstigen Unterauftragsverarbeiter, sämtliche in Anlage 2 zu dieser Vereinbarung aufgeführt, gilt die Zustimmung des Auftraggebers mit Abschluss dieser Vereinbarung als erteilt.

(4) Weitere Unterauftragsverarbeiter

Die weitere Auslagerung auf Unterauftragsverarbeiter oder der Wechsel bestehender Unterauftragsverarbeiter sind unter den Voraussetzungen des § 6 Abs. 2 dieser Vereinbarung auch ohne gesonderte Zustimmung des Auftraggebers zulässig, soweit ATOSS dem Auftraggeber die Auslagerung auf (andere) Unterauftragsverarbeiter eine angemessene Zeit vorab in Textform anzeigt und die nachfolgenden Regelungen erfüllt sind. Alternativ kann ATOSS eine Website oder eine andere Art der Benachrichtigung bereitstellen, welche alle Unterauftragsverarbeiter, die auf die personenbezogenen Daten des Auftraggebers zugreifen, sowie die von ihnen erbrachten begrenzten oder ergänzenden Dienstleistungen auflistet. Mindestens zwei Wochen vor der Genehmigung des Zugriffs auf personenbezogene Daten durch einen neuen Unterauftragsverarbeiter wird ATOSS den Auftraggeber hierüber benachrichtigen und, falls einschlägig, die Website aktualisieren. Durch die Benachrichtigung räumt ATOSS dem Auftraggeber das Recht ein, der Änderung innerhalb von zwei Wochen aus berechtigten Gründen zu widersprechen. Widerspricht der Auftraggeber nicht innerhalb dieser Widerspruchsfrist, gilt die Zustimmung als erteilt. Auf Verlangen des Auftraggebers wird ATOSS sämtliche erforderlichen Informationen zur Verfügung stellen, um nachzuweisen, dass der Unterauftragsverarbeiter alle datenschutzrechtlichen Anforderungen des dieser Vereinbarung erfüllt. Für den Fall, dass der Auftraggeber der Auslagerung widerspricht, kann ATOSS wählen, ob er den Unterauftragsverarbeiter nicht beauftragt oder die Leistungsvereinbarung mit einer Frist von zwei Monaten schriftlich kündigt.

(5) Geltung der Bestimmungen dieser Vereinbarung auch für Unterauftragsverarbeiter

Auf Verlangen des Auftraggebers wird ATOSS dem Auftraggeber Informationen über relevante datenschutzrechtliche Verpflichtungen des Unterauftragsverarbeiters zur Verfügung stellen, die unter anderem die Gewährung des erforderlichen Zugangs zu den einschlägigen Vertragsdokumenten umfasst. ATOSS wird seine Unterauftragsverarbeiter regelmäßig überprüfen und wird auf Aufforderung des Auftraggebers die Einhaltung des Datenschutzrechts und der Verpflichtungen des Unterauftragsverarbeiters aus dem mit ihm abgeschlossenen Auftragsverarbeitungsvertrag bestätigen. Nur bei Vorliegen berechtigter Gründe ist der Auftraggeber berechtigt, ATOSS Weisungen zu erteilen, weitere Prüfungen vorzunehmen, die ATOSS im Rahmen des Zulässigen durchführen wird.

§ 7 - Pflichten und Rechte des Auftraggebers; Unterstützung des Auftraggebers durch ATOSS

Der Auftraggeber ist zur Wahrung der Rechte der betroffenen Person (Art. 12 ff. DS-GVO bzw. §§ 32 ff. BDSG), 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. Bei der Einhaltung der Pflichten unterstützt ATOSS den Auftraggeber. In diesem Zusammenhang stellt er ihm sämtliche Informationen bereit, soweit der Auftraggeber über diese Informationen nicht selbst verfügt. ATOSS ist nicht verpflichtet, Informationen zum Zweck der Unterstützung zu beschaffen, über die er seinerseits nicht verfügt. ATOSS unterstützt den Auftraggeber wie folgt:

(1) Wahrung der Rechte der betroffenen Personen

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

(2) Technische und organisatorische Maßnahmen

ATOSS 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 zeitnahe Feststellung von relevanten Verletzungsereignissen ermöglichen.

Der Auftraggeber hat hierbei insbesondere in geeigneter und dem Schutzbedarf angemessener Form sicherzustellen, dass die von ATOSS 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 ATOSS ist ATOSS 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 ATOSS verursacht wurden, hat ATOSS 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) Protokollierung der Verarbeitungsvorgänge

Beide Parteien verpflichten sich, Zugriffe auf die in der Datenbank der von ATOSS bereitgestellten Software-Lösungen befindlichen Auftragsdaten jeweils ausschließlich unter Verwendung separater Benutzerkennungen vorzunehmen. Dies setzt voraus, dass der Auftraggeber ATOSS entsprechende separate Benutzerkennungen zur Verwendung im Rahmen der Auftragsverarbeitung zuteilt bzw. an deren Erstellung im erforderlichen Umfang mitwirkt. ATOSS wird Zugangskennungen ausschließlich den betreffenden Personen sowie ggf. einem für die Verwaltung der Zugangskennungen verantwortlichen Mitarbeiter zugänglich machen und diese durch geeignete und angemessene Maßnahmen gegen unbefugte Einsichtnahme und / oder Verwendung sichern.

(b) Kontrollhandlungen bei ATOSS oder Auftraggeber

(aa) ATOSS 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 bei ATOSS 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 bei ATOSS ausgesetzt ist, hat ihn ATOSS nach besten Kräften zu unterstützen.

(c) Datenschutz-Folgenabschätzung

Soweit eine gesetzliche Pflicht des Auftraggebers zur Erstellung einer Datenschutz-Folgenabschätzung besteht, unterstützt ihn ATOSS 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 bei ATOSS anzumelden sind, von der Einhaltung der gesetzlichen und in dieser Vereinbarung übernommenen Verpflichtungen von ATOSS in den Geschäftsbetrieb zu den üblichen 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 von ATOSS sein.

ATOSS kann der Überprüfung durch einen externen Prüfer widersprechen, wenn der vom Auftraggeber ausgewählte Prüfer in einem Wettbewerbsverhältnis zu ATOSS steht.

(b) Dokumentation

ATOSS stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten von ATOSS nach Art. 28 DS-GVO im Rahmen der Auftragsverarbeitung überzeugen kann. ATOSS 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

Die Kontaktdaten des Datenschutzbeauftragten befinden sich in der Anlage 1 (Technische und organisatorische Maßnahmen).

(6) Sonstige Unterstützungsleistungen

Für weitere Unterstützungsleistungen, die nicht in den Leistungsvereinbarungen enthalten oder nicht auf ein Fehlverhalten von ATOSS zurückzuführen sind, kann ATOSS eine gesonderte Vergütung beanspruchen.

§ 8 - Löschung oder Rückgabe nach Abschluss der Verarbeitung

(1) Wahlrecht

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarungen – hat ATOSS 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 erforderlich sind, die Fertigung und Zwischenspeicherung von Screenshots von Auftragsdaten im Rahmen der parametrierten Standard-Software auf IT-Systemen von ATOSS zum Zwecke der Fehleranalyse betreffend vom Auftraggeber gemeldete Fehlfunktionen 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 ATOSS 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

(1) Externe Haftung

Der Auftraggeber und ATOSS haften jeweils für Schäden betroffener Personen gemäß Art. 82 DS-GVO (externe Haftung).

(2) Interne Haftung

Jede Partei ist berechtigt, von der jeweils anderen Partei, den Teil der Entschädigung zurückzufordern, der dem Teil der Verantwortung des anderen für den Schaden entspricht (interne Haftung).

(3) Haftungsvereinbarung

Hinsichtlich der internen Haftung und ohne Auswirkung auf die externe Haftung gegenüber den betroffenen Personen vereinbaren die Parteien, dass ungeachtet der hierin enthaltenen Bestimmungen die Haftung von ATOSS für die Verletzung dieses Auftragsverarbeitungsvertrages den in der Leistungsvereinbarung vereinbarten Haftungsbeschränkungen unterliegt. Der Auftraggeber stellt ATOSS von allen Ansprüchen und Schäden frei, die über die Haftungsbeschränkungen des Rahmenvertrags hinausgehen, sofern ATOSS diese im Zusammenhang mit Ansprüchen der betroffenen Personen aufgrund einer angeblichen Verletzung von Bestimmungen der DS-GVO oder dieses Auftragsverarbeitungsvertrages erlitten hat.

§ 10 - Schlussbestimmungen

(1) Ersetzungsklausel; Änderungen und Ergänzungen

(a) Diese Vereinbarung tritt mit Unterzeichnung der der Datenverarbeitung im Auftrag zugrundeliegenden Leistungsvereinbarung 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 Anlage 1 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 bei ATOSS durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter, ist ATOSS 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.