Auftragsverarbeitungsvereinbarung
("AVV")

Inhaltsverzeichnis

Präambel 1
§ 1 Gegenstand dieser AVV 2
§ 2 Beschreibung der Verarbeitung 3
§ 3 Technische und organisatorische Maßnahmen 3
§ 4 Weisungsbefugnis 4
§ 5 Verpflichtung zur Vertraulichkeit 5
§ 6 Beauftragung von Unterauftragsverarbeitern 5
§ 7 Pflichten und Rechte des KUNDEN; Unterstützung des KUNDEN durch ATOSS 7
§ 8 Löschung oder Rückgabe nach Abschluss der Verarbeitung 9
§ 9 Haftung und Recht auf Schadensersatz 9
§ 10 Schlussbestimmungen 9

AVV-Anhangsverzeichnis:

AVV-Anhang I **Beschreibung der Verarbeitung**
AVV-Anhang II **Technische und organisatorische Maßnahmen**
AVV-Anhang III **Liste der genehmigten Unterauftragsverarbeiter**

Präambel

Diese Auftragsverarbeitungsvereinbarung ("**AVV**") ist in dem Vertrag über die Bereitstellung sowohl von ATOSS Produkten On Premises als auch für einen ATOSS CLOUD SERVICE (einzeln und zusammen nachfolgend "**ATOSS PRODUKTE**" genannt) und damit zusammenhängender sonstiger Services sowie Dienstleistungen enthalten (nachfolgend auch "**VERTRAG**" bezeichnet). Diese AVV ist somit zugleich ein fester Bestandteil eines schriftlich (auch in elektronischer Form) geschlossenen Vertrags zwischen der vertragsschließenden ATOSS-Gesellschaft (als Auftragsverarbeiter - nachfolgend "**ATOSS**" genannt) und dem KUNDEN. Beide, ATOSS und der KUNDE werden nachfolgend gemeinsam "**PARTEIEN**" oder einzeln "**PARTEI**" bezeichnet. Die PARTEIEN sind sich einig, dass der KUNDE auch seinen VERBUNDENEN UNTERNEHMEN die Nutzung von lizenzierten ATOSS PRODUKTEN gemäß den Bestimmungen des jeweiligen VERTRAGS gestatten kann. Da in einem solchen Fall auch personenbezogene Daten von VERBUNDENEN UNTERNEHMEN des KUNDEN durch ATOSS verarbeitet werden, gilt diese AVV für die folgenden Szenarien:

- Der KUNDE ist der einzige Verantwortliche im Hinblick auf die personenbezogenen

Daten, die ATOSS für die Auftragsverarbeitung zugänglich gemacht werden.

- Neben dem KUNDEN nutzen die lizenzierten ATOSS PRODUKTE auch seine VERBUNDENEN UNTERNEHMEN; der KUNDE und seine VERBUNDENEN UNTERNEHMEN sind jeweils allein oder gemeinsam Verantwortliche.
- Der KUNDE ist hinsichtlich der eigenen personenbezogenen Daten Verantwortlicher und hinsichtlich der personenbezogenen Daten seiner VERBUNDENEN UNTERNEHMEN Auftragsverarbeiter. Aus der Sicht seiner VERBUNDENEN UNTERNEHMEN ist ATOSS ein Unterauftragsverarbeiter des KUNDEN.
- Der KUNDE ist nur Auftragsverarbeiter seiner VERBUNDENEN UNTERNEHMEN und ATOSS ist Unterauftragsverarbeiter hinsichtlich der personenbezogenen Daten.

Ungeachtet der vorstehenden Fallgruppen ist der KUNDE unter dieser AVV stets der zentrale und direkte operative Ansprechpartner für ATOSS. Soweit ATOSS in diesem Zusammenhang personenbezogene Daten verarbeitet, gelten hierfür die Bedingungen dieser AVV.

Für die Zurverfügungstellung der ATOSS PRODUKTE gemäß dem VERTRAG ist der Einsatz von Unterauftragsverarbeitern notwendig. Insoweit ist dem KUNDEN bewusst, dass ATOSS die ATOSS PRODUKTE nicht ohne Unterauftragsverarbeiter erbringen kann. Der Einsatz der Unterauftragsverarbeiter richtet sich nach Ziffer 6 dieser AVV.

Hinweis zur Geschlechterneutralität: Die gewählten Formulierungen gelten uneingeschränkt für die weiteren Geschlechter.

§ 1 Gegenstand dieser AVV

1. Zweck und Anwendungsbereich: Mit dieser AVV soll die Einhaltung von Art. 28 Abs. 3 und Abs. 4 DSGVO sichergestellt werden.

   Die im VERTRAG aufgeführten PARTEIEN haben dieser AVV zugestimmt, um die Einhaltung von Art. 28 Abs. 3 und Abs. 4 DSGVO zu gewährleisten.

   Diese AVV gilt für die Verarbeitung personenbezogener Daten gemäß AVV-Anhang I.

   Die AVV-Anhänge I bis III sind Bestandteil dieser AVV.

   Werden in dieser AVV die in der DSGVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung. Im Übrigen gelten die Definitionen aus dem VERTRAG in dieser AVV entsprechend.

   Diese AVV ist im Lichte der Bestimmungen der DSGVO auszulegen. Diese AVV darf nicht in einer Weise ausgelegt werden, die den in der DSGVO vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

2. Pflichten des KUNDEN: Diese AVV gilt unbeschadet den Verpflichtungen, denen der Verantwortliche gemäß der DSGVO unterliegt.

§ 2 Beschreibung der Verarbeitung

Den konkreten Leistungsumfang vereinbaren die PARTEIEN im VERTRAG. Die in Betracht kommenden Leistungen umfassen regelmäßig Sachverhalte im Sinne der Auftragsverarbeitung von personenbezogenen Daten. Das gilt entsprechend für eine (Fern-) Prüfung und (Fern-) Wartung automatisierter Verfahren oder dem Einsatz von Datenverarbeitungsanlagen, sofern dabei ein Zugriff auf personenbezogene Daten des KUNDEN nicht ausgeschlossen werden kann.

Die Einzelheiten der relevanten Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für welche die personenbezogenen Daten im Auftrag verarbeitet werden, sind in **AVV-Anhang I - Beschreibung der Verarbeitung** aufgeführt.

§ 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 DSGVO). ATOSS versichert, dass ATOSS die Regelungen der Art. 28 Abs. 3 lit. c), 32 DSGVO 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 Auftragsverarbeitung, 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 ergreift mindestens die in **AVV-Anhang II - technische und organisatorische Maßnahmen** aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten.

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 AVV festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen sind zu dokumentieren und dem KUNDEN auf geeignete Weise anzuzeigen (z.B. per E-Mail oder über ein über die Website von ATOSS zugängliches Online-Portal). Durch diese Anzeige räumt ATOSS dem KUNDEN die Möglichkeit ein, diesen Änderungen innerhalb von sechs (6) Wochen in Schrift- oder Textform zu widersprechen. Der KUNDE ist nur dann zum Widerspruch berechtigt, wenn die Änderungen nicht den Anforderungen der § 3 Ziffer 1 und § 3 Ziffer 2 dieser AVV entsprechen. Widerspricht der KUNDE den Änderungen nicht oder nicht berechtigt innerhalb der Widerspruchsfrist, gilt die Zustimmung zu den Änderungen nach Fristablauf als erteilt.

Im Falle eines berechtigten Widerspruchs kann ATOSS den Teil der Leistungserbringung aussetzen, der von dem berechtigten Widerspruch des KUNDEN betroffen ist.

§ 4 Weisungsbefugnis

1. Dokumentierte Weisung: ATOSS verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des KUNDEN, es sei denn, ATOSS ist nach Unionsrecht oder nach dem Recht des Mitgliedstaats, dem ATOSS unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt ATOSS dem KUNDEN diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der VERTRAG einschließlich dieser AVV stellt eine dokumentierte Weisung des KUNDEN dar.

2. Bestimmtheit und Form der Weisung: Soweit nicht ausdrücklich in dieser AVV abweichend vereinbart, sind Weisungen bestimmt zu erteilen (Gebot der Weisungsklarheit). Weisungen müssen schriftlich oder in Textform erteilt werden.

3. Umsetzbarkeit der Weisung: ATOSS wird dem KUNDEN innerhalb einer angemessenen Zeit in Textform mitteilen, soweit die Umsetzung der Weisung im Rahmen der Standardfunktionalitäten selbstständig vom KUNDEN konfiguriert werden kann.

   Weisungen des KUNDEN, die eine Abweichung zu den im VERTRAG oder dieser AVV festgelegten Leistungen darstellen, werden als Antrag auf Vertragsänderung behandelt. Die Pflichten aus dem VERTRAG und dieser AVV bleiben während des Zeitraums der Prüfung unberührt. ATOSS wird sich im Rahmen des Zumutbaren bemühen, Weisungen des KUNDEN, die als Antrag auf Vertragsänderung zu qualifizieren sind, umzusetzen, soweit sie insbesondere datenschutzrechtlich erforderlich und technisch möglich sind bzw. keine Änderungen der ATOSS PRODUKTE erfordern. ATOSS wird den KUNDEN vorab in Textform informieren, falls erkennbar ist, dass ATOSS für die Prüfung und Umsetzung der Weisung ein Mehraufwand und/oder zusätzliche Kosten entstehen und nach Rücksprache mit dem KUNDEN ein Angebot für Beauftragung von kostenpflichtigen Dienstleistungen für die weitere Prüfung und Umsetzung der Weisung übermitteln. Für den Fall, dass keine Einigung über eine Vertragsänderung zustande kommt, bleiben die Pflichten aus dem VERTRAG bestehen.

   Von ATOSS bestätigte Weisungen werden in gemeinsamer Abstimmung der PARTEIEN innerhalb eines angemessenen Zeitraums umgesetzt.

4. Benachrichtigung bei Rechtswidrigkeit: ATOSS informiert den KUNDEN unverzüglich, wenn ATOSS der Auffassung ist, dass vom KUNDEN erteilte Weisungen gegen die DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. ATOSS ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den KUNDEN bestätigt oder geändert wird.

5. Rechte der betroffenen Personen: Auskünfte an von der Auftragsverarbeitung betroffene Personen oder an DRITTE darf ATOSS nur nach vorheriger Weisung des KUNDEN erteilen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an ATOSS wendet, wird ATOSS dieses Ersuchen unverzüglich an den KUNDEN weiterleiten.

6. Regress: Sollte ATOSS infolge der Umsetzung einer rechtswidrigen Weisung einem begründeten Haftungsanspruch ausgesetzt sein, kann ATOSS sich insoweit beim KUNDEN schadlos halten.

§ 5 Verpflichtung zur Vertraulichkeit

1. Daten- und Fernmeldegeheimnis: ATOSS und jede ATOSS unterstellte Person, die Zugang zu den verarbeiteten personenbezogenen Daten hat, sind zur Vertraulichkeit verpflichtet, insbesondere gemäß den Bestimmungen der Art. 5 Abs. 1 lit. f), Art. 28 Abs. 3 lit. b), Art. 29 und Art. 32 Abs. 4 DSGVO sowie des § 3 TTDSG. Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung dieser AVV 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 personenbezogenen Daten befugten Personen mit den einschlägigen Bestimmungen zum Datengeheimnis und Fernmeldegeheimnis vertraut sind.

§ 6 Beauftragung von Unterauftragsverarbeitern

1. [bleibt aus redaktionellen Gründen frei]

2. Voraussetzungen der Zulässigkeit der Beauftragung: Die Beauftragung von Unterauftragsverarbeitern ist nur nach Zustimmung des KUNDEN möglich.

a) Allgemeine Anforderungen: Beauftragt ATOSS einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des KUNDEN), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für ATOSS gemäß dieser AVV gelten. ATOSS stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen ATOSS entsprechend dieser AVV und gemäß der DSGVO unterliegt.

   ATOSS stellt dem KUNDEN auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann ATOSS den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

   ATOSS haftet gegenüber dem KUNDEN in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit ATOSS geschlossenen VERTRAG nachkommt. ATOSS benachrichtigt den KUNDEN, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten in Bezug auf Leistungen gegenüber dem KUNDEN nicht erfüllt.

b) Unterauftragsverarbeiter in Drittstaaten: Jede Übermittlung von Daten durch ATOSS an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des KUNDEN (vgl. § 4) oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaates, dem ATOSS unterliegt, und muss mit Kapitel V der DSGVO im Einklang stehen.

   In Fällen, in denen ATOSS einen Unterauftragsverarbeiter gemäß diesem § 6 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des KUNDEN) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, dürfen ATOSS und sein Unterauftragsverarbeiter die Einhaltung von Kapitel V der DSGVO sicherstellen, indem

sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Art. 46 Absatz 2 der DSGVO erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

3. Gegenwärtige Unterauftragsverarbeiter: ATOSS besitzt die allgemeine Genehmigung des KUNDEN für die Beauftragung von Unterauftragsverarbeitern, die in **AVV-Anhang III - Liste der genehmigten Unterauftragsverarbeiter** zu dieser AVV aufgeführt sind. Bezogen auf den Einsatz dieser Unterauftragsverarbeiter gilt die Zustimmung des KUNDEN mit Abschluss dieser AVV als erteilt.

4. Weitere Unterauftragsverarbeiter: Die weitere Auslagerung auf Unterauftragsverarbeiter oder der Wechsel bestehender Unterauftragsverarbeiter sind unter den Voraussetzungen des § 6 Ziffer 2 dieser AVV auch ohne ausdrückliche Zustimmung des KUNDEN zulässig, soweit ATOSS dem KUNDEN die Auslagerung auf (andere) Unterauftragsverarbeiter eine angemessene Zeit vorab (z.B. per E-Mail oder über ein über die Website von ATOSS zugängliches Online-Portal) anzeigt und die nachfolgenden Regelungen erfüllt sind: ATOSS unterrichtet den KUNDEN mindestens 6 Wochen im Voraus über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem KUNDEN damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Widersprüche gegen diese Änderungen erheben zu können.

   ATOSS stellt dem KUNDEN eine aktualisierte Liste zur Verfügung, welche alle Unterauftragsverarbeiter, die auf die personenbezogenen Daten des KUNDEN zugreifen, sowie die von ihnen erbrachten begrenzten oder ergänzenden Dienstleistungen auflistet. Durch die Anzeige räumt ATOSS dem KUNDEN die Möglichkeit ein, diesen Änderungen innerhalb von sechs (6) Wochen zu widersprechen.

   Der KUNDE ist nur dann zum Widerspruch berechtigt, wenn die Änderungen nicht den Anforderungen des § 6 Ziffer 2 dieser AVV entsprechen. Widerspricht der KUNDE den Änderungen nicht oder nicht berechtigt in Schrift- oder Textform innerhalb der Widerspruchsfrist, gilt die Zustimmung zu den Änderungen nach Fristablauf als erteilt. Im Falle eines berechtigten Widerspruchs kann ATOSS den Einsatz des geänderten Unterauftragsverarbeiters aussetzen, der von dem berechtigten Widerspruch des KUNDEN betroffen ist. Für den Fall, dass der KUNDE dem Einsatz auch nach Rücksprache mit ATOSS widerspricht, kann ATOSS wählen, ob er den Unterauftragsverarbeiter nicht beauftragt oder den VERTRAG mit einer Frist von zwei (2) Monaten schriftlich kündigt. Diese Regelung ergänzt die Kündigungsregelung im VERTRAG.

5. Geltung der Bestimmungen dieser AVV auch für Unterauftragsverarbeiter: Auf Verlangen des KUNDEN wird ATOSS dem KUNDEN 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 KUNDEN die Einhaltung des Datenschutzrechts und der Verpflichtungen des Unterauftragsverarbeiters aus dem mit ihm abgeschlossenen Auftragsverarbeitungsvertrag bestätigen. Nur bei Vorliegen berechtigter Gründe ist der KUNDE berechtigt, ATOSS Weisungen zu erteilen, weitere Prüfungen vorzunehmen, die ATOSS im Rahmen des Zulässigen durchführen wird.

§ 7 Pflichten und Rechte des KUNDEN; Unterstützung des KUNDEN durch ATOSS

Der KUNDE ist zur Wahrung der Rechte der betroffenen Person (Art. 12 ff. DSGVO), zur Ergreifung technischer und organisatorischer Maßnahmen, zur Meldung und Benachrichtigung bei Datenschutzverletzungen, zur Zusammenarbeit mit der Aufsichtsbehörde (Art. 32 bis 36 DSGVO) sowie zur Qualitätssicherung (Art. 28 Abs. 1 DSGVO) verpflichtet. Bei der Einhaltung der Pflichten unterstützt ATOSS den KUNDEN. In diesem Zusammenhang stellt ATOSS ihm sämtliche Informationen bereit, soweit der KUNDE über diese Informationen nicht selbst verfügt. ATOSS ist nicht verpflichtet, Informationen zum Zweck der Unterstützung zu beschaffen, über die ATOSS seinerseits nicht verfügt. ATOSS unterstützt den KUNDEN wie folgt:

1. Wahrung der Rechte der betroffenen Personen: ATOSS unterrichtet den KUNDEN unverzüglich über jeden Antrag, den er von einer betroffenen Person des KUNDEN erhalten hat. ATOSS beantwortet den Antrag nicht selbst. Die Wahrung der Rechte der betroffenen Personen obliegt dem KUNDEN. Soweit erforderlich, unterstützt ATOSS den KUNDEN im Falle der Ausübung von Rechten durch die betroffenen Personen.

2. Technische und organisatorische Maßnahmen: ATOSS unterstützt den KUNDEN 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 KUNDE hat hierbei insbesondere in geeigneter und dem Schutzbedarf angemessener Form sicherzustellen, dass die von ATOSS bereitgestellten ATOSS PRODUKTE 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 personenbezogenen Daten durch ATOSS ist ATOSS verpflichtet, den KUNDEN 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 AVV, gleich ob diese durch den KUNDEN, einen Dritten oder ATOSS verursacht wurden, hat ATOSS den KUNDEN unverzüglich und vollständig über Zeitpunkt, Art und Umfang der betroffenen personenbezogenen Daten zu informieren. Dem KUNDEN sind sämtliche relevante Informationen zur Erfüllung der Meldepflicht gegenüber der Aufsichtsbehörde unverzüglich zur Verfügung zu stellen. Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

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 bei ATOSS oder beim KUNDEN:

(aa) ATOSS informiert den KUNDEN unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf den VERTRAG beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung von personenbezogenen Daten bei der Auftragsverarbeitung bei ATOSS ermittelt.

(bb) Soweit der KUNDE 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.

b) Datenschutz-Folgenabschätzung: Soweit eine gesetzliche Pflicht des KUNDEN 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 KUNDEN.

5. Dokumentation und Einhaltung:

a) Prüfungen: Die PARTEIEN müssen die Einhaltung dieser Klauseln nachweisen können. ATOSS bearbeitet Anfragen des KUNDEN bezüglich der Verarbeitung von Daten gemäß dieser AVV unverzüglich und in angemessener Weise. ATOSS stellt dem KUN-DEN alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in dieser AVV festgelegten und unmittelbar aus der DSGVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des KUNDEN gestattet ATOSS ebenfalls die Prüfung der unter dieser AVV fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Prüfung kann der KUNDE einschlägige Informationen und Zertifizierungen von ATOSS berücksichtigen.

Der KUNDE kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. ATOSS kann der Prüfung durch einen unabhängigen Prüfer widersprechen, wenn der vom KUNDEN ausgewählte Prüfer in einem Wettbewerbsverhältnis zu ATOSS steht oder nicht auf die Einhaltung der Vertraulichkeit verpflichtet wurde.

Die Kosten von Prüfungen gemäß § 7 (5) lit. a) sind vom KUNDEN zu tragen.

b) Dokumentation: Der Nachweis der Dokumentation der technischen und organisatorischen Maßnahmen kann insbesondere auch durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder durch einen geeigneten Nachweis über ein IT-Sicherheits- oder Datenschutzaudit erfolgen.

c) Datenschutzbeauftragter: Die Kontaktdaten des Datenschutzbeauftragten sind in dem **AVV-Anhang II - Technische und organisatorische Maßnahmen** genannt.

§ 8 Löschung oder Rückgabe nach Abschluss der Verarbeitung

1. Löschung oder Rückgabe: Die Löschung und Rückgabe der personenbezogenen Daten richtet sich nach den Bestimmungen in **AVV-Anhang I - Beschreibung der Verarbeitung** und den vertraglichen Bestimmungen.
2. [bleibt aus redaktionellen Gründen frei]
3. Aufbewahrungsfristen: Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch ATOSS entsprechend den jeweiligen gesetzlichen Aufbewahrungsfristen über das Ende dieser AVV hinaus aufzubewahren. ATOSS kann sie zu seiner Entlastung nach Ende dieser AVV dem KUNDEN übergeben.
4. Kosten: Zusätzliche Kosten, die durch von diesem § 8 Ziffer 1 abweichende bzw. darüberhinausgehende Weisungen des KUNDEN entstehen, hat der KUNDE zu tragen.

§ 9 Haftung und Recht auf Schadensersatz

1. Die Parteien haften unter dieser AVV gemäß den gesetzlichen Bestimmungen der DSGVO.
2. [bleibt aus redaktionellen Gründen frei]
3. [bleibt aus redaktionellen Gründen frei]

§ 10 Schlussbestimmungen

1. Ersetzungsklausel; Änderungen und Ergänzungen:

a) Diese AVV tritt mit Abschluss des VERTRAGS in Kraft und ersetzt mit ihrem Inkrafttreten in ihrem Anwendungsbereich sämtliche etwaig bestehenden Vereinbarungen zur Auftragsverarbeitung zwischen den PARTEIEN.

b) Soweit nicht ausdrücklich abweichend geregelt, bedürfen Änderungen und Ergänzungen zu dieser AVV sowie alle Nebenabreden zu ihrer Wirksamkeit der Schriftform oder Textform.

c) Unbeschadet der Bestimmungen in § 3 Ziffer 3 (Aktueller Stand der Technik und technische Anpassungen) sowie § 6 Ziffer 4 (Weitere Unterauftragsverarbeiter) ist ATOSS berechtigt, die Bestimmungen dieser AVV zu ändern oder zu ergänzen, soweit hierdurch das bei Vertragsschluss vereinbarte Äquivalenzverhältnis in Bezug auf wesentliche Vertragsbestandteile nicht negativ berührt wird und die Änderungen für den KUNDEN zumutbar sind. Die Anpassungsbefugnis erstreckt sich hierbei insbesondere auf Änderungen in Bezug auf (i) technische Entwicklungen, (ii) Änderungen der rechtlichen Rahmenbedingungen, (iii) die Beseitigung einer nachträglich entstandenen Äquivalenzstörung oder (iv) die Beseitigung von Regelungslücken (z. B. bei unvorhersehbaren, veränderten Umständen). ATOSS wird den KUNDEN über die geplanten Änderungen vorab informieren. Die Änderungen gelten als vom KUNDEN angenommen, wenn er diesen nicht innerhalb von sechs (6) Wochen nach der Änderungsmitteilung gegenüber ATOSS in Schrift- oder Textform widerspricht. In der Änderungsmitteilung weist ATOSS den KUNDEN auch auf die vorgesehene Bedeutung seines Verhaltens hin.

2. Nichtanwendbarkeit der Allgemeinen Geschäfts- / Einkaufsbedingungen des KUNDEN: Es besteht zwischen den PARTEIEN Einigkeit darüber, dass "Allgemeine Geschäftsbedingungen" und / oder „Allgemeine Einkaufsbedingungen“ des KUNDEN auf diese AVV keine Anwendung finden.
3. Ausschluss des Zurückbehaltungsrechts: Die Einrede des Zurückbehaltungsrechts wird hinsichtlich der verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen.
4. [bleibt aus redaktionellen Gründen frei]
5. Verpflichtung zur Information im Fall der Gefährdung der personenbezogenen Daten: Im Fall der Gefährdung der personenbezogenen Daten bei ATOSS durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter, ist ATOSS verpflichtet, den KUNDEN darüber unverzüglich zu informieren.
6. Gerichtstand: Es gelten die Bestimmungen in § 10 Ziffer 7 dieser AVV.
7. Rechtsbehelfe: Für Rechtsbehelfe einer betroffenen Person gegen ATOSS als Auftragsverarbeiter gelten die anwendbaren Datenschutzbestimmungen. Für Rechtsbehelfe der PARTEIEN aus oder im Zusammenhang mit dieser AVV gelten in Bezug auf die Rechtswahl und den Gerichtsstand die Bestimmungen des VERTRAGES.
8. Salvatorische Klausel: Sollten einzelne Teile dieser AVV 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.

AVV-Anhang I

- Beschreibung der Verarbeitung -

1. **Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden**

   Abhängig vom KUNDEN, kommen folgende durch die Verarbeitung betroffene Personen in Betracht:

   - Beschäftigte
   - Beamtinnen und Beamte sowie Anwärterinnen und Anwärter der Länder
   - Tarifbeschäftigte und zu ihrer Berufsausbildung Beschäftigte

2. **Kategorien personenbezogener Daten, die verarbeitet werden**

   Welche Kategorien personenbezogener Daten im jeweiligen VERTRAG tatsächlich verarbeitet werden, richtet sich maßgeblich nach der vom KUNDEN jeweils gewählten Konfiguration und Parametrisierung sowie der vereinbarten Modulauswahl.

   Ergänzende Informationen können den jeweiligen Vertragsunterlagen und/oder anderen bereitgestellten Informationen (z.B. im Rahmen der Nutzung unserer Website, digitalen Kundenlounge) entnommen werden.

   Relevante personenbezogene Datenkategorien können insbesondere sein:

a) 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, E-Mail, 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 und 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 oder Stempelungen inkl. Uhrzeit und Ort der Buchung oder 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

b) 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

c) 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

d) 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 oder Verlassen von Zonen inkl. Uhrzeit und Ort der Buchung

e) Systembezogene Informationen

- Systemzugangsinformationen
- Informationen über Berechtigungen für bestimmte Objekte und Interaktionen als Nutzer des Systems
- Internet-Protokoll (IP), Paket Informationen, einschließlich URLs, Zeitstempel, telemetrische Daten, Ports in Bezug auf die Nutzung von ATOSS Cloud Services
- Browser Informationen (Browser User Agents, Log-Daten) in Bezug auf die Nutzung von ATOSS Cloud Services
- Zuletzt verwendete Systemeinstellungen und Präferenzen
- Angemeldete Systemnutzer
- Anmeldeversuche
- Protokolle über Nutzerinteraktionen, die Daten im System verändern.

f) Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

3. Art der Verarbeitung

a) Verarbeitungstätigkeiten

Die Leistungen von ATOSS können - wie in dem jeweiligen VERTRAG mit dem KUNDEN näher beschrieben - insbesondere folgende Verarbeitungstätigkeiten umfassen:

- Customizing i.S.v. Parametrisierung der ATOSS PRODUKTE (insbesondere Unterstützung beim Anlegen der Mitarbeiterstammdaten in der Datenbank der dem KUNDEN von ATOSS zur Nutzung bereitgestellten Standard-Software, beim Einrichten von Arbeitszeitmodellen und Zeitkonten usw.) und Anpassung bzw. Scripting von Standard-Schnittstellen;
- Softwarepflege betreffend die ATOSS PRODUKTE (insbesondere Unterstützung bei Software-Releasewechseln, dem Einspielen von kontinuierlichen Modifikationen sowie bei der Behebung von gemeldeten Fehlfunktionen);
- Hotline-Leistungen betreffend die ATOSS PRODUKTE (insbesondere die Annahme von Informationen oder die Unterstützung bei der Analyse für 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 ATOSS PRODUKTE.
- Managed-Service-Leistungen betreffend die Administration von personenbezogenen Daten gemäß des im VERTRAG festgelegten Umfangs (insbesondere aktive Unterstützung bei der Administration von personenbezogenen Daten von Mitarbeitern des KUNDEN in dem von ATOSS bereitgestellten ATOSS PRODUKT)

Die Verarbeitungstätigkeiten – sei es ganz oder teilweise – können dabei erfolgen:

- vor Ort beim KUNDEN (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 KUNDEN);
- per Fernzugriff über eine gesicherte VPN-Verbindung und eine vom KUNDEN bereitgestellte geeignete Softwarelösung zum Fernzugriff (z.B. VPN, Desktop Sharing), die auf aktuellen Windows-Server Betriebssystemen lauffähig ist (inkl. notwendiger Lizenz) oder im Falle von ATOSS PRODUKTEN per Fernzugriff über eine gesicherte VPN-Verbindung zu den IT-Systemen des Betreibers der Cloudinfrastrukturen, auf denen die personenbezogenen Daten des KUNDEN verarbeitet werden.

In allen Fällen ist eine lesende und schreibende Zugriffsmöglichkeit auf die in den ATOSS PRODUKTEN integrierte Datenbank und ggf. auf die beim KUNDEN damit verbundenen weiteren informationsverarbeitenden Systeme, die personenbezogene Daten enthalten, nicht auszuschließen.

b) Sachliche Beschränkung der Verarbeitung

Eine über diese AVV hinausgehende Verarbeitung von personenbezogenen Daten des Auftraggebers ist ATOSS nicht gestattet. Eine Verarbeitung für andere Zwecke, insbesondere die eigenmächtige Weitergabe von Auftragsdaten an DRITTE, ist nicht zulässig. ATOSS ist verpflichtet, die personenbezogenen Daten verschiedener Kunden getrennt zu verarbeiten.

c) Örtliche Beschränkung

Die Erbringung der unter einem VERTRAG vereinbarten Auftragsverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) oder in der Schweiz (CH) statt.

Erfolgt die Datenverarbeitung in einem Drittland, d.h. außerhalb der EU, des EWR oder der Schweiz, stellt ATOSS sicher, dass vor der Datenübermittlung die besonderen Voraussetzungen der Art. 44 ff. DSGVO sowie die Maßgaben dieser AVV erfüllt sind.

d) Protokollierung der Verarbeitungsvorgänge

Die PARTEIEN verpflichten sich, Zugriffe auf die in den ATOSS PRODUKTEN integrierte Datenbank und den dort verarbeiteten personenbezogenen Daten ausschließlich unter Verwendung separater Nutzerkennungen vorzunehmen. Dies setzt voraus, dass der KUNDE für ATOSS entsprechende separate Nutzerkennungen zur Verwendung im Rahmen der Auftragsverarbeitung zuteilt und an deren Einrichtung im erforderlichen Umfang mitwirkt. ATOSS wird diese Nutzerkennungen ausschließlich dem für die Durchführung der Leistungen erforderlichen Personal zugänglich machen und diese durch geeignete und angemessene Maßnahmen gegen unbefugte Einsichtnahme und Verwendung sichern.

4. Zweck(e) der Verarbeitung

ATOSS verarbeitet die personenbezogenen Daten des KUNDEN nur für die im VERTRAG genannten spezifischen Zwecke, sofern keine weiteren Weisungen seitens des KUNDEN an ATOSS erteilt werden. Grundlegender Zweck der Verarbeitung ist die Gewährleistung der Funktionalität und der Aktualität der dem KUNDEN von ATOSS zur Nutzung zur Verfügung gestellten ATOSS PRODUKTE.

5. Dauer der Verarbeitung

Die vom KUNDEN überlassenen personenbezogenen Daten werden von ATOSS für die im VERTRAG zwischen den PARTEIEN angegebene Dauer verarbeitet. Diese entspricht üblicherweise der Vertragslaufzeit des VERTRAGS, einschließlich etwaiger nachvertraglicher Pflichten. Ist die Vertragslaufzeit nicht festgelegt, beginnt die Dauer der Auftragsverarbeitung mit der Aufnahme der geschuldeten Leistungen und endet mit Beendigung der Pflichten bei Vertragsbeendigung. Die Löschpflicht besteht nicht, sofern nach dem Unionsrecht oder dem anwendbaren nationalen Recht eine Verpflichtung zu Speicherung der Daten besteht, worunter namentlich abgabenrechtliche oder handelsbilanzielle Aufbewahrungspflichten fallen.

***

AVV – Anhang II

– Technische und organisatorische Maßnahmen –

Alle Geschäftsstellen sowie alle Konzerngesellschaften der ATOSS Software SE nutzen die gesamte IT-Infrastruktur des Unternehmenssitzes in München. Sämtliche Tätigkeiten - auch via remote - werden ausschließlich mit IT-Ressourcen und Betriebsmitteln durchführt, die von der ATOSS Software SE gestellt und zentral kontrolliert werden. Das interne Rechenzentrum befindet sich in München.

Im Folgenden sind die technischen und organisatorischen Maßnahmen von ATOSS in Bezug auf die internen IT-Systeme und internen Geschäftsprozesse der Geschäftsstellen und der Konzerngesellschaften der ATOSS Software SE aufgeführt. Abhängig vom jeweiligen ATOSS Standort sind (geringfügige) Abweichungen möglich.

I. VERTRAULICHKEIT

1. Physische Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Bürogebäuden, Arbeitsplätzen und internen Datenverarbeitungsanlagen zu verwehren.

I.1.1	**Bürogebäude und Arbeitsplätze**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Einbruchmeldeanlage (EMA) ☒ Elektronisches Schließsystem ☒ Zutrittstechniken (z.B. RFID, PIN oder mechanische Schlüssel) mit personenspezifischer Vergabe ☒ Mechanisches Schließsystem für das Gebäude / die Büroräume ☒ Chipkarten ☒ Klingelanlage mit Kamera ☒ Videoüberwachung der Eingangsbereiche ☒ Bewegungsmelder, Überfallmelder ☒ Wachdienst	☒ Standortverantwortliche ☒ Ausgabe von Schlüsseln wird protokolliert mittels Ausgabe- und Rückgabeprotokolle ☒ Sicherheitszonen ☒ Empfangs-/Besucherbereiche ☒ Beschränkung des Zutritts für betriebsfremde Personen (z. B. Besucherinnen und Besucher) ☒ Besucher-Management-Prozess, inkl. (De-) Registrierung, Besucherausweise, Begleitung durch Mitarbeitende ☒ Sorgfalt bei Auswahl des Wachdienstes

I.1.2	Internes Rechenzentrum	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Betrieb des internen Rechenzentrums durch ATOSS IT-Abteilung ☒ Einbruchmeldeanlage (EMA) ☒ Elektronisches Schließsystem ☒ Zutrittstechnik (z.B. RFID und mechanische Schlüssel) mit personenspezifischer Vergabe ☒ Videoüberwachung	☒ Begrenzung der Schlüsselausgabe und Einschränkung der Zutrittsrechte für den Zugang zum Rechenzentrum auf privilegiertes Personal der ATOSS IT-Abteilung ☒ Ausgabe von Schlüsseln wird protokolliert mittels Ausgabe- und Rückgabeprotokolle ☒ Besucher-Management-Prozess, inkl. (De-) Registrierung, Besucherausweise, Begleitung durch Mitarbeitende

2. Digitale Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass interne Datenverarbeitungsanlagen und Informationen von Unbefugten genutzt werden können.

I.2	Interne Systeme, Applikationen, Notebooks, Smartphones	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Anbindung der Geschäftsstellen und Konzerngesellschaften per verschlüsseltem Server-Netzwerk (Domänen-Controller) ☒ Nutzung nur von ATOSS intern freigegebenem IT-Equipment und Applikationen, Systemen ☒ Verbot von BYOD ☒ BIOS-gestützte Festplatten-Authentifizierung von mobilen Endgeräten (z.B. Notebooks, Tablets) ☒ Gehäuseverriegelung ☒ Login mit personalisierten Benutzer-Accounts + Passwort ☒ Login mit privilegierten Accounts + Passwort + 2. Faktor ☒ Protokollierung der An- und Abmeldungen, Anmeldeversuche ☒ Automatische passwortgeschützte Desktop- / Bildschirmsperre ☒ Verbot mit Ausnahmevorbehalt für Nutzung von hardwareverschlüsselten Wechselmedien (z.B. USB-Sticks mit 256-bit-AES) ☒ Einsatz VPN-Anbindung bei Fernzugriffen ☒ Mobil Device Management	☒ Benutzer- und Berechtigungsmanagement ☒ Passwortmanagement ☒ Begrenzung von Anmeldeversuchen und automatischer Zugangssperrung ☒ Richtlinie zum Umgang mit Passwörtern und Zugangsschutz ☒ Vorgaben zum manuellem Sperren ☒ Passworthistorie ☒ Richtlinie zum Umgang mit Unternehmenswerten, inkl. Löschung/Vernichtung ☒ Richtlinie zum Datenschutz und Informationssicherheit in der Organisation ☒ Richtlinie Smartphones ☒ Richtlinie Social Media ☒ Kontrolle und Aufbewahrung der Protokolle ☒ Sicherheitsupdates ☒ Penetrationstests (jährlich) ☒ Incident Management ☒ Change Management ☒ IT-Notfall Management

	☒ Verschlüsselung von Festplatten (256-bit AES) ☒ Viren-, Spyware-, Malwareschutz ☒ SIEM ☒ Firewalls ☒ Spamfilter ☒ Proxy (inkl. Virenschutz) ☒ Intrusion Prevention System (IPS) ☒ Passwort-Server ☒ Verschlüsselung des Datentransfers (z.B. BIOS-Passwörter, VPN-Anbindungen, Ironkeys inkl. Virenscanner) ☒ Applikationen werden auf die technische Möglichkeit geprüft, Schnittstellen zu verhindern oder zu schließen	

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung von internen Datenverarbeitungssystemen Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Informationen zugreifen können, und dass Informationen bei der Verarbeitung, Nutzung und nach der Speicherung nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können.

I.3	**Informationen (unabhängig, ob in elektronischer oder physischer Form)**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Zugriffsberechtigungen werden durch ein zentrales Microsoft Active Directory bzw. eine firmeneigene Domäne definiert, koordiniert und kontrolliert. ☒ Protokollierung von Zugriffen auf Anwendungen (Eingabe, Änderung und Löschung von Zugriffsberechtigungen) ☒ Datenschutztresor ☒ Mitarbeiterschließfächer ☒ Vernichtung von elektronischen Datenträgern durch einen externen Entsorgungsdienstleister (Standard DIN 66399-3) ☒ Entsorgung von klassifizierten Dokumenten in verschlossenen Datentonnen ☒ Aktenvernichtung und Leerung durch externen Entsorgungsdienstleister	☒ Rollenbasiertes Berechtigungskonzept ☒ Benutzer- und Berechtigungsmanagement (inkl. Vorgaben bei Eintritt, Funktionswechsel, Ausscheiden) ☒ Beschränkte Anzahl von Administratoren / von privilegierten Benutzer-Accounts ☒ Richtlinie zum Umgang mit Unternehmenswerten, inkl. Löschung/Vernichtung ☒ Richtlinie Clean Desk ☒ Ausgabe von Schließfächerschlüsseln wird protokolliert mittels Ausgabe- und Rückgabeprotokolle ☒ Kontrolle und Aufbewahrung der Protokolle ☒ Sorgfalt bei Auswahl des Entsorgungsdienstleisters ☒ Gesonderte Zugangspunkte für externe IT-Systeme

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten logisch oder physikalisch getrennt verarbeitet werden.

I.4	**Systemkontrolle / Speicherkontrolle**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Trennung von personenbezogenen Daten des KUNDEN im Sinne einer Auftragsdatenverarbeitung und von sonstigen internen Geschäftsinformationen ☒ Trennung von Produktiv- und Testumgebungen ☒ Mandantenfähigkeit relevanter Applikationen ☒ Test von Software / Hardware erfolgt in isolierten virtuellen Umgebungen (Sandboxing)	☒ Übermittlungsverbot von personenbezogenen Daten des KUNDEN im Sinne einer Auftragsdatenverarbeitung außerhalb festgelegter Übermittlungs- und Kommunikationswege an ATOSS ☒ Festlegung von internen Datenbankrechten ☒ Interne Domänenverwaltung ☒ Interne Netzwerk--Topologiepläne ☒ Change Management

II. INTEGRITÄT

1. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Informationen in interne Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

II.1	**Protokollierungen / Logging (z.B. Betriebssysteme, Netzwerke, Firewalls, Datenbanken, Applikationen)**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Technische Protokollierung von An- und Abmeldungen von Benutzern auf ATOSS internen Datenverarbeitungssystemen ☒ Zentrale Speicherung der Protokolldaten in Bezug auf ATOSS interne Datenverarbeitungssysteme ☒ Uhrensynchronisation/Timeserver	☒ Rollenbasierte Eingabe-, Änderungs- und Löschbeschränkungen werden über das Benutzer- und Berechtigungsmanagement gesteuert und kontrolliert ☒ Aufbewahrung von Protokollen nach den gesetzlichen Vorgaben ☒ Manuelle oder automatisierte Kontrolle der Protokolle

2. Weitergabekontrolle

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

II.2	Elektronische und physische Datenübertragungen	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ E-Mail-Verschlüsselung (S/MIME, TLS, Zertifikate) ☒ Contentfilter für E-Mail und Web ☒ Telefonie-Verschlüsselung (SAML, TLS, Zertifikate) ☒ Einsatz von VPN auf mobilen Endgeräten ☒ Verbot mit Sondererlaubnisvorbehalt für Nutzung von hardwareverschlüsselten Wechselmedien (z.B. USB-Sticks mit 256-bit AES) ☒ Verschlossene Briefkästen ☒ Nutzung von festgelegten Kommunikations- und Übermittlungswegen	☒ Richtlinie zur Informationsübertragungen von und nach extern ☒ Entnahme von Briefpost ausschließlich durch unternehmenseigenes Empfangspersonal ☒ Persönliche Verteilung bei externer Briefpost ☒ Persönliche Verteilung bei interner, (sehr) vertraulich gekennzeichneter Briefpost / Dokumenten ☒ Warenlieferungen nur innerhalb Anlieferungszonen mit persönlicher Entgegenahme ☒ Definierte Vorgaben bei Fernzugriffen (siehe ergänzende Informationen unten*) ☒ Verhinderung / Löschung von Übermittlungen von nicht-anonymisierten personenbezogenen Daten des KUNDEN außerhalb abgestimmter und festgelegter Übertragungswege (siehe ergänzende Informationen*)

***Ergänzende Informationen:**

Die Übermittlung von nicht-anonymisierten personenbezogenen Daten des KUNDEN darf nur durch den KUNDEN selbst, entweder über die eingerichteten Übertragungswege in den ATOSS Cloud Services oder auf den kundeneigenen IT-Systemen erfolgen. Eine Übersendung nicht-anonymisierten personenbezogenen Daten des KUNDEN über E-Mailverkehr an Empfänger bei ATOSS ist zu unterlassen.

Für die Erbringung von Parametrisierung-, Softwarepflege- und Hotline-Leistungen mit Zugriffen auf die lizenzierte Kundeninstallation muss der KUNDE die Zugriffs- und Weitergabekontrolle durch entsprechende Konfigurationen im User Management sicherstellen:

- Die (De-) Registrierung von Nutzern (einschließlich von ATOSS Hotline- und Customer Service Beratern) kann nur vom KUNDEN vorgenommen und nach eigens von ihm festgelegten Prüfzyklen zu überwacht werden.
- Parametrisierung-, Softwarepflege- und Hotline-Leistungen mit Zugriffen auf die lizenzierte Kundeninstallation auf den IT-Systemen des KUNDEN vor Ort oder per Fernzugriff bedürfen einer vorherigen Nutzerberechtigung bzw. Freischaltung durch den KUNDEN.
- Parametrisierung-, Softwarepflege- und Hotline-Leistungen per Fernzugriff erfolgen ausschließlich über gesicherte Verbindungen und unter Berücksichtigung der in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.
- Soweit erforderlich, wirken ATOSS Hotline- und Customer Service Berater auf Weisungen des KUNDEN an der Konfiguration technischer Kontrolleinrichtungen mit. Sofern dabei Fernzugriffe auf den kundeneigenen IT-Systemen erfolgen sollen, stellt der KUNDE eine geeignete Softwarelösung zum Fernzugriff (z.B. VPN, Desktop Sharing), die auf aktuellen Windows Server Betriebssystemen lauffähig ist (inkl. notwendiger Lizenz), bereit. Fernzugriffe werden dabei kontrolliert und betreut durch die ATOSS Remote Access Services (RAS) Abteilung.
- Der KUNDE ist befähigt, Fernzugriffe mitzuverfolgen und jederzeit abzubrechen.
- Personenbezogene Daten des KUNDEN dürfen nur auf ausdrückliche Weisung des KUNDEN auf Wechseldatenträgern von ATOSS gespeichert werden. Entsprechende Kopien werden nach Abschluss des konkreten Zugriffs durch ATOSS gelöscht.

III. VERFÜGBARKEIT

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

I.1.1	**Bürogebäude und Arbeitsplätze, Hardware, IT-Ressourcen**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Brandschutzvorkehrungen (z.B. Feuer- und Rauchmeldeanlagen) ☒ Feuertüren und Fluchtwege ☒ Notstromversorgung ☒ Zertifizierte und abgenommene Elektroinstallationen (inklusive Überspannungsschutz und bereichsorientierte	☒ Elektrochecks aller elektronischen Geräte gemäß Prüfzyklus vom Hersteller ☒ Regelmäßige Funktionsprüfungen ☒ Durchführung von Wartungen und Pflege durch Dienstleister ☒ Sorgfalt bei Auswahl von Dienstleistern ☒ Dokumentation der Switch-Ports

	Energieverteilung) ☒ Synchronisierte USV-Anlage ☒ Telekommunikations- und Provideranbindungen über mindestens zwei Glasfaseranbindungen und separater Übertragungstechnik ☒ Redundante Anbindung aller wichtigen Komponenten ☒ Elektrorevision (VDS) ☒ Strukturierte Verkabelung ☒ Separater "Netzwerkschrank" für Anbindung und Netzwerk ☒ Computergesteuertes Überwachungssystem der Verbindungen	☒ Sicherheitsupdates ☒ Incident Management ☒ Change Management ☒ IT-Notfall Management
I.1.2	**Internes Rechenzentrum**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Brandschutzvorkehrungen (u.a. durch eigenen Brandschutzabschnitt, Anbindung an Brandmeldezentrale, Rauchmelder) ☒ Feuchtigkeitssensoren ☒ Rauchansaugsystem (RAS) ☒ Redundante Klimatisierung ☒ Netzersatzanlage (NEA, Dieselgenerator) ☒ Redundante unterbrechungsfreie Stromversorgung ☒ Getrennte Stromkreise ☒ Telekommunikations- und Provideranbindungen über mindestens zwei Glasfaseranbindungen und separater Übertragungstechnik. ☒ Redundante Anbindung aller wichtigen Komponenten ☒ Elektrorevision (VDS) ☒ Strukturierte LAN-Verkabelung ☒ Separater "Netzwerkschrank" für Anbindung und Netzwerk ☒ Computergesteuertes Überwachungssystem der Verbindungen ☒ Redundante interne Speichersysteme ☒ Sicherungsbänder, Aufbewahrung der Backups in redundantem Speichersystem im Rechenzentrum ☒ Sicherungsdienst an einem anderen Ort	☒ Backup und Desaster Recovery Konzept ☒ Geographische Trennung der Backupspeicherorte vom Ort des primären Servers ☒ Datensicherungen erfolgen mehrfach täglich (für relevante interne IT-Systeme) ☒ Backups sind verschlüsselt ☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse ☒ Backups werden über Echtzeitspiegelung erstellt ☒ Transport der Sicherungsbänder durch Sicherheitsdienst ☒ Sorgfalt bei Auswahl des Sicherungsdienstes ☒ Sicherheitsupdates ☒ Incident Management ☒ Change Management ☒ IT-Notfall Management

IV. VERSCHLÜSSELUNG UND PSEUDONYMISIERUNG

☒ Die elektronische Übermittlung von E-Mailverkehr erfolgt verschlüsselt.
☒ Die elektronische Übermittlung von personenbezogenen Daten darf nur auf verschlüsselten und festgelegten Übermittlungs- und Kommunikationswegen erfolgen. Eine Übermittlung von nicht-anonymisierten, personenbezogenen KUNDENDATEN (z. B. Testdaten, Mitarbeiterstammdaten etc.) auf vorab nicht gemeinsam festgelegten Übermittlungs- und Kommunikationswegen ist nicht zulässig.
☒ Die Speicherung von personenbezogenen Daten erfolgt auf IT-Systemen des Kunden oder in den ATOSS Cloud Services.
☒ Die Speicherung von personenbezogenen Daten im ATOSS internen Geschäftsbetrieb erfolgt verschlüsselt.
☒ Alle Daten auf mobilen Rechner und Speichermedien werden verschlüsselt.
☒ Alle produktiv eingesetzten Verschlüsselungstechnologien entsprechen dem *Stand der Technik**
☒ Für die relevanten IT-Systeme ist die Verwaltung des Schlüsselmaterials definiert und dokumentiert.
☒ Transportverschlüsselung wird ausschließlich Ende-zu-Ende implementiert.
☒ Ein Regelwerk mit Anforderungen an Verschlüsselungsstärke, -algorithmus und Verwaltung der Schlüssel ist implementiert.
☒ Pseudonymisierung personenbezogener Daten durch Einwegfunktionen.
☒ Pseudonymisierung durch Zuordnungstabellen, diese sind von der übrigen Datenverarbeitung getrennt.

**Definition* - Stand der Technik umfasst die bis zum jeweiligen Zeitpunkt gewonnenen technischen Erkenntnisse, die Eingang in die betriebliche Praxis gefunden haben und allgemein anerkannt sind.

V. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

1. Datenschutz-Management

IV.1	**Einhaltung und Überprüfung der Maßnahmen**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen wird mind. jährlich durchgeführt (externes DSGVO-Audit) ☒ Toolgestützte Kontrolle von regelmäßigen Mitarbeiterschulungen und Teilnahmen	☒ Interne Datenschutzbeauftragte (Kontaktdaten sind auf der ATOSS Website bekanntgegeben) ☒ Mitarbeiterschulungskonzept ☒ Regelmäßige Sensibilisierung der Mitarbeitenden (mindestens jährlich) ☒ Einhaltung der Informationspflichten nach Art. 13 und Art. 14 DSGVO ☒ Formalisierter Prozess zur Bearbeitung von Datenschutzanfragen und Meldungen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörden)

		☒ Datenschutz-Folgenabschätzungen (DSFA) werden bei Bedarf durchgeführt. ☒ Einbindung der Datenschutzbeauftragten in internen und externen Datenschutzangelegenheiten

2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des KUNDEN verarbeitet werden können.

IV.3	**Genehmigte Unterauftragsverarbeiter**	
	Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Zertifizierte, dokumentierte Sicherheitsmaßnahmen von (Hosting) Service Providern	☒ Sorgfalt bei Auswahl von ATOSS Unterauftragsverarbeitern ☒ Vorlage und Prüfung von Nachweisen über Kontrollmaßnahmen und DSGVO-Konformität von (Hosting) Service Providern (z.B. Prüfreporte, Zertifikate) ☒ Abschluss einer Auftragsverarbeitungsvereinbarung ☒ Dokumentation von Weisungen ☒ Verpflichtung von ATOSS Unterauftragsverarbeitern auf Vertraulichkeit und das Datengeheimnis ☒ Abschluss von EU Standard-Vertragsklauseln oder anderen Garantien nach Art. 46 DSGVO (sofern erforderlich) ☒ Fortlaufende Überprüfungen von Unterauftragsverarbeitern in Bezug auf Datenschutz und Informationssicherheit ☒ Verpflichtung von Unterauftragsverarbeitern im Falle von Drittlandstransfers, dass ein Transfer Impact Assessment bzgl. der weiteren Unter-Unterauftragnehmer durchgeführt wurde und, dass das Ergebnis dieser Bewertung positiv / DSGVO-konform ist.

***

AVV-Anhang III

- Liste der genehmigten Unterauftragsverarbeiter -

ATOSS besitzt die allgemeine Genehmigung des KUNDEN für die Beauftragung von Unterauftragsverarbeitern, die in diesem AVV-Anhang III aufgeführt sind.

ATOSS kann während der Dauer der Verarbeitung von personenbezogenen Daten zwischen den in diesem AVV-Anhang III aufgeführten und damit vom KUNDEN bereits genehmigten Unterauftragsverarbeitern jederzeit nach eigenem Ermessen auswählen und wechseln. ATOSS behält sich vor, für die Verarbeitung von personenbezogenen Daten nicht jeden der nachfolgend aufgeführten Unterauftragsverarbeiter einzusetzen.

Unternehmen	**Registrierte Adresse**	**Tätigkeitsbeschreibung**	**Bemerkung**
ATOSS Gesellschaften			
ATOSS Software SE (Deutschland)	Rosenheimer Str. 141h 81671 München **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	ATOSS Konzerngesellschaft (soweit nicht Vertragspartner)
ATOSS CSD Software GmbH	Rodinger Str. 19 93413 Cham **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	ATOSS Konzerngesellschaft (soweit nicht Vertragspartner)
ATOSS Software Ges.m.b.H.	Ungargasse 64-66 Stiege 3 Top 503 1030 Wien **Österreich**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	ATOSS Konzerngesellschaft (soweit nicht Vertragspartner)
ATOSS Software AG (Schweiz)	Schärenmoosstr. 77 8052 Zürich **Schweiz**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	ATOSS Konzerngesellschaft (soweit nicht Vertragspartner)
SC ATOSS Software SRL	Calea Torontalului 69 Timisoara 300668 **Rumänien**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	ATOSS Konzerngesellschaft (soweit nicht Vertragspartner)

Unternehmen	Registrierte Adresse	Tätigkeitsbeschreibung	Bemerkung
Unterauftragsverarbeiter, die Hilfsdienste zur Unterstützung von professionellen Services erbringen			
Accenture N.V/SA	Rue Picard/ Picardstraat 11 Boîte/Bus 100 1000 Brüssel **Niederlande**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
AIKAVA GmbH	Amselstr. 15 93413 Cham **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
b.it³ Business Software+IT GmbH	Birkenstr. 2 5300 Salzburg / Hallwang **Österreich**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Bosch Sicherheitssysteme GmbH	Robert-Bosch-Ring 5 85630 Grasbrunn **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Capgemini Deutschland GmbH	Potsdamer Platz 5 10785 Berlin **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Delaware Consulting CV	Kapel ter Bede 86, 8500 Kortrijk **Belgien**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
DELOITTE Consulting GmbH	Dammtorstraße 12 20149 Hamburg **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)

Unternehmen	**Registrierte Adresse**	**Tätigkeitsbeschreibung**	**Bemerkung**
EMPAL GmbH	Bügelestorstr. 7/2 74354 Besigheim **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Fourtexx GmbH	Grünewalder Str. 28 42657 Solingen **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
GZ Gute Zeiten e. K.	Geistenbecker Str. 50 41199 Mönchengladbach **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
KEGA	Madame Curiestraat 24 2171 TW Sassenheim **Niederlande**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Moretime oHG	Sedanstr. 13 93055 Regensburg **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
OPTIMO WFM BV	Wijersstraat 1 3811 MZ Amersfoort **Niederlande**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Ringer Zeiterfassung GmbH & Co. KG	Vollmerstraße 17 88400 Biberach a.d. Riss **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)

Unternehmen	**Registrierte Adresse**	**Tätigkeitsbeschreibung**	**Bemerkung**
Robert Schickbauer (On time Consulting)	Schoarerbergstr. 43 5302 Henndorf am Wallersee **Österreich**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
SOFT-CONSULT Häge GmbH	Riedheimer Straße 5 89129 Langenau **Deutschland**	Parametrierung, Softwarepflege-Leistungen, Hotline-Leistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Unterauftragsverarbeiter, die Hilfsdienste zur Unterstützung bei der Einrichtung von Schnittstellen erbringen			
SHAPEiN GmbH	Ruländerweg 10 60168 Wiesloch **Deutschland**	Schnittstellendienstleister inkl. Softwarepflegeleistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Pentos AG	Landsberger Str. 110 80339 München **Deutschland**	Schnittstellendienstleister inkl. Softwarepflegeleistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
HR Force EDV-Beratung GmbH	Wambachergasse 10 1130 Wien **Österreich**	Schnittstellendienstleister inkl. Softwarepflegeleistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
EMPLEOX GmbH (ehemals KWP INSIDE HR GmbH)	Ferdinand-Braun-Str. 24 74074 Heilbronn **Deutschland**	Schnittstellendienstleister inkl. Softwarepflegeleistungen	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)

Unternehmen	Registrierte Adresse	Tätigkeitsbeschreibung	Bemerkung
Unterauftragsverarbeiter, die Hilfsdienste zur Unterstützung bei der Einrichtung von Hardware erbringen			
OSC Business Xpert GmbH	Werftstr. 15 30163 Hannover **Deutschland**	Dienstleister für Anbindung von Hardware-Komponenten inkl. Support-/ Pflegeleistungen und Parametrierung	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Unterauftragsverarbeiter, die Hilfsdienste im Fall eines ATOSS CLOUD SERVICE erbringen			
Microsoft Ireland Operations Limited	South County Business Park Leopardstown Dublin 18 **Irland**	Hosting-Provider inklusive Managed IT-Services (Hosting und Betrieb der Cloud-Infrastruktur)	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Telekom Deutschland GmbH	Landgrabenweg 151 53227 Bonn **Deutschland**	Hosting-Provider inklusive Managed IT-Services (Hosting und Betrieb der Cloud-Infrastruktur)	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
UMB AG	Müllerenstr. 3 8604 Volketswil **Schweiz**	Hosting-Provider inklusive Managed IT-Services (Hosting und Betrieb der Cloud-Infrastruktur)	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)
Google Ireland Limited	Gordon House Barrow Street Dublin 4 **Irland**	Bei ATOSS Mobile Workforce Management (zur Erbringung eines Push-nachrichten-Services: Übermittlung von Push-Nachrichten aus dem Modul ATOSS Mobile Workforce Management sowie Mobile Employee Self Service User und Mobile Manager Self Service User an Nutzer mit mobilen Endgeräten	Unterauftragsverarbeiter (soweit zur Leistungserbringung erforderlich)

***