Anlage 2

Auftragsdatenverarbeitungsvereinbarung

Vereinbarung

über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 11 Bundesdatenschutzgesetz (BDSG) („Vereinbarung“)

zwischen

Ringer Zeiterfassungssysteme

Alte Biberacher Straße 5

88447 Warthausen

und

[…]

- nachfolgend ”KUNDE” genannt -

- nachfolgend zusammen ”Vertragsparteien” genannt -

Inhaltsverzeichnis

§1 Gegenstand der Vereinbarung

Gegenstand der Vereinbarung ist die Erhebung bzw. Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag im Zusammenhang mit der Bereitstellung von gehosteten IT-Services im Rechenzentrum bezogen auf die Allgemeinen Geschäftsbedingungen für Hosting und Betrieb von ATOSS-Produkten („Hauptvertrag“). Die Vereinbarung gilt entsprechend für (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Es wird ausdrücklich festgehalten, dass allein der Auftraggeber gegenüber der Ringer Zeiterfassungssysteme weisungsbefugt ist und sämtliche Maßnahmen und Weisungen seiner Kunden gegenüber der Ringer Zeiterfassungssysteme koordiniert. Sofern in dieser Vereinbarung vom „Auftraggeber“ gesprochen wird, meint dies den KUNDEN in seiner Eigenschaft als Auftraggeber gegenüber der Ringer Zeiterfassungssysteme.

§2 Bereitstellung von Daten durch den KUNDEN

1. Die Ringer Zeiterfassungssysteme erhält, soweit im Rahmen der Leistungserbringung nach dem Hauptvertrag erforderlich, Zugriff auf folgende personenbezogene Daten (insbesondere

dadurch, dass der KUNDE ihr die Daten bereitstellt oder ihr einen Zugriff auf die Daten ermöglicht):

Personaldaten (Stamm- und Bewegungsdaten) des KUNDEN, die durch die Ringer Zeiterfassungssysteme ggf. unter Einbindung deren Hosting-Subunternehmer für den KUNDEN in dem gehosteten Personaleinsatzplanungs-, Zeitwirtschafts- und Zutrittskontrollsystem ASES, verarbeitet werden

insbesondere

Mitarbeiterstammdaten und zeitwirtschaftliche Informationen

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

- Anträge für Abwesenheiten inkl. Genehmigungsverlauf und –stand
- Anträge für Arbeitszeit- oder Dienstplanungs- relevante Vorgänge inkl. Genehmigungsverlauf und –stand
- Anstehende und erledigte Aufgaben
- Informationen über vom System versandte Email- und SMS-Benachrichtigungen

- Informationen des Zutrittsmanagements
  - Informationen über Zutrittsberechtigungen für bestimmte Zonen und Zeiträume
  - Zugangskennungen
  - 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 System-Benutzer
  - Anmeldeversuche
  - Protokolle über Benutzerinteraktionen, die Daten im System verändern

Die Verarbeitung von Daten erfolgt wie im Hauptvertrag beschrieben.

§3 Datenerhebung, -verarbeitung oder -nutzung durch die Ringer Zeiterfassungssysteme

Die Ringer Zeiterfassungssysteme erbringt für den KUNDEN bezogen auf die in § 2 genannten Daten Leistungen, die im Hauptvertrag beschrieben sind.

§4 Prüfung, Wartung, Fernzugriff, Datenlöschung (Entsorgung)

1. Prüfungs- und Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen – auch solche im Wege des Fernzugriffs – werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, mit vorheriger schriftlicher Zustimmung des KUNDEN ausgeführt. Art und Umfang der Prüfungs- und Wartungsarbeiten bzw. der Fernzugriffe sind in § 2 und § 3 dieser Vereinbarung bzw. dem Hauptvertrag beschrieben.
   Die Mitarbeiter der Ringer Zeiterfassungssysteme verwenden Identifizierungs- und Verschlüsselungsverfahren, wie in Annex 2 zu dieser Vereinbarung beschrieben.
2. Prüfungs- und Wartungsarbeiten, auch solche im Weg des Fernzugriffs, werden von der Ringer Zeiterfassungssysteme dem KUNDEN vorab mit angemessener Frist schriftlich angekündigt und bei Durchführung dokumentiert und protokolliert. Der KUNDE ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der KUNDE -soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.
3. Die Ringer Zeiterfassungssysteme wird von den ihr eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfange – auch in zeitlicher Hinsicht - Gebrauch machen, als dies für die ordnungsgemäße Durchführung der

beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

4. Soweit bei der Leistungserbringung durch die Ringer Zeiterfassungssysteme nach dem Hauptvertrag Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z.B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten des KUNDEN notwendig ist, wird die Ringer Zeiterfassungssysteme die vorherige Zustimmung des KUNDEN einholen. Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Zustimmung des KUNDEN. Bei Datenabzug der Wirkbetriebsdaten wird die Ringer Zeiterfassungssysteme diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers datenschutzgerecht löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des KUNDEN oder auf solchem der Ringer Zeiterfassungssysteme verwendet werden, sofern die vorherige Zustimmung des KUNDEN vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des KUNDEN auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.
5. Prüfungs- und Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere die vorstehend beschriebenen Tätigkeiten wie Löschen, Transport, Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird die Ringer Zeiterfassungssysteme die technischen und organisatorischen Maßnahmen wie in den Leistungsbeschreibungen/Einzelverträgen oder in Annex 2 beschrieben, ergreifen.

§5 Rechte und Pflichten des KUNDEN

1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der KUNDE verantwortlich. Der KUNDE wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit die Ringer Zeiterfassungssysteme die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.
2. Der KUNDE hat das Recht, Weisungen über Art und Umfang der Datenverarbeitung zu erteilen. Der KUNDE erteilt alle Aufträge oder Teilaufträge und Weisungen schriftlich oder per Telefax oder per E-Mail. Die Ringer Zeiterfassungssysteme wird den KUNDEN unverzüglich informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. In diesem Fall ist die Ringer Zeiterfassungssysteme berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis diese durch den KUNDEN bestätigt oder geändert wird. Zusätzliche Weisungen bedürfen der Schriftform. Zusätzliche Weisungen und Maßnahmen, die über diese vertraglich vereinbarten Leistungen hinausgehen, sind bei Mehraufwand für die Ringer Zeiterfassungssysteme gesondert zu vergüten.
3. Der KUNDE kann, nach seiner Wahl, die Einhaltung der Vorschriften über den Datenschutz durch die Einholung von Auskünften, Selbstzertifizierungen oder Zertifizierungen anerkannter Prüfer bei der

Ringer Zeiterfassungssysteme im Hinblick auf die Datenverarbeitung nach dieser Vereinbarung kontrollieren. Wenn und soweit der begründete Verdacht eines Verstoßes der Ringer Zeiterfassungssysteme gegen die Regelungen dieser Vereinbarung besteht oder eine zuständige Datenschutzbehörde weitergehende Kontrollen fordert, ist die Ringer Zeiterfassungssysteme selbst bzw. in Begleitung eines Kundenvertreters auch zur Einsichtnahme in die gespeicherten Daten, die zur Verarbeitung der Daten genutzten IT-Systeme und Datenverarbeitungsprogramme sowie sonstigen Vor-Ort- Kontrollen berechtigt, um die Einhaltung der Regelungen dieser Vereinbarung zu überprüfen. Der KUNDE kann das Ergebnis der Kontrollen dokumentieren. Der KUNDE kann die Kontrollen selbst durchführen oder durch einen von ihm beauftragten Dritten auf seine Kosten durchführen lassen. Der Dritte ist mit Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Dritte im Sinne dieser Vereinbarung dürfen keine Vertreter von Wettbewerbern der Ringer Zeiterfassungssysteme sein. Der KUNDE wird Kontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen.

§6 Rechte und Pflichten der Ringer Zeiterfassungssysteme

1. Die Ringer Zeiterfassungssysteme verarbeitet die Daten ausschließlich im Rahmen des Hauptvertrages, dieser Vereinbarung und nach schriftlichen Weisungen des KUNDEN. Sie verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, die ihr überlassenen Daten an Dritte weiterzugeben. Die Ringer Zeiterfassungssysteme ist verpflichtet, die Daten verschiedener Kunden des Auftraggebers pro Kunden getrennt zu verarbeiten.
2. Die Ringer Zeiterfassungssysteme wird die LEISTUNGEN von den in Annex 1 vereinbarten Leistungsstandorten aus und ggf. durch die genehmigten Subunternehmer (vgl. § 9 unten) erbringen. Wenn die Ringer Zeiterfassungssysteme die geschuldeten Leistungen ganz oder teilweise von einem anderen Standort innerhalb der EU/dem EWR erbringen möchte, wird die Ringer Zeiterfassungssysteme vorab die schriftliche Zustimmung durch den KUNDEN einholen. Entsprechendes gilt für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch die Ringer Zeiterfassungssysteme, z.B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung. Bei einer Leistungserbringung außerhalb Deutschlands aus Ländern, die Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, wird der KUNDE seine Zustimmung zur Verlagerung oder des Einsatzes eines Subunternehmers nicht unbillig verweigern, wenn sich diese Verlagerung nicht negativ auf den Datenschutz auswirkt und die Ringer Zeiterfassungssysteme dem KUNDEN vorab Details zur Verlagerung und der vom neuen Standort erbrachten Leistungen schriftlich mitgeteilt hat.
3. Eine Verlagerung des Ortes der Leistungserbringung in Länder, die nicht Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den

Europäischen Wirtschaftsraum sind, ist nicht gestattet.

4. Unterlagen mit personenbezogenen Daten und Dateien, mit Ausnahme der aufgrund gesetzlicher Verpflichtung der Ringer Zeiterfassungssysteme weiter vorzuhaltenden Daten, werden erst nach Weisung/Zustimmung durch den KUNDEN vernichtet. Gleiches gilt für Test- und Ausschussmaterial. Soweit sich Speichermedien im Besitz des KUNDEN befinden, wird der KUNDE vor einer etwaig vorgesehenen Übergabe an die Ringer Zeiterfassungssysteme oder deren Unterauftragnehmer alle personenbezogenen Daten datenschutzgerecht löschen. Sollte dies dem KUNDEN nicht möglich sein, wird er die Ringer Zeiterfassungssysteme rechtzeitig schriftlich informieren. Die Ringer Zeiterfassungssysteme ist dann berechtigt, diese personenbezogenen Daten im Auftrag des KUNDEN zu löschen. Soweit nicht ausdrücklich anders vereinbart, wird der Aufwand der Löschung der Ringer Zeiterfassungssysteme gesondert vergütet.
5. Nach Abschluss der vertraglichen Arbeiten (inkl. Wind Down Period) oder früher nach Aufforderung durch den KUNDEN, spätestens jedoch innerhalb von fünf (5) Arbeitstagen nach Beendigung des Hauptvertrages, hat die Ringer Zeiterfassungssysteme sämtliche in ihren Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, einschließlich personenbezogener Daten, die im Zusammenhang mit dem Hauptvertrag stehen, auf eigene Kosten dem KUNDEN auszuhändigen oder nach vorheriger Zustimmung durch den KUNDEN datenschutzgerecht zu vernichten. Gleiches gilt für Test-, Back-up- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung dem KUNDEN vorzulegen.
6. Der KUNDE hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten bei der Ringer Zeiterfassungssysteme zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte der Ringer Zeiterfassungssysteme erfolgen. Die Vor-Ort-Kontrolle ist mit angemessener Frist durch den KUNDEN anzukündigen.
7. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, können durch die Ringer Zeiterfassungssysteme entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden.
8. Die Ringer Zeiterfassungssysteme informiert den KUNDEN unverzüglich nach Kenntniserlangung über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen oder Verletzungen dieser Vereinbarung, gleich ob diese durch den KUNDEN, Dritte oder die Ringer Zeiterfassungssysteme verursacht wurden, bei Verstößen gegen die in dieser Vereinbarung getroffenen Festlegungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des KUNDEN.
9. Es ist der Ringer Zeiterfassungssysteme bekannt, dass nach § 42a Bundesdatenschutzgesetz (BDSG) Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Stellt die Ringer Zeiterfassungssysteme daher

fest, oder begründen Tatsachen die Annahme, dass von ihr für den KUNDEN verarbeitete

- besondere Arten personenbezogener Daten (§ 3 Absatz 9 BDSG) oder
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten oder
- Bestands- oder Nutzungsdaten (§ 15 a TMG)

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat die Ringer Zeiterfassungssysteme den KUNDEN unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E- Mail) zu informieren. Die Information soll eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Die vorstehende Verpflichtung gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verstöße gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit Daten des Auftraggebers. Die Ringer Zeiterfassungssysteme hat im Benehmen mit dem KUNDEN angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den KUNDEN oder dessen Kunden Pflichten nach § 42a BDSG treffen, hat die Ringer Zeiterfassungssysteme hierbei angemessen zu unterstützen.

10. Die Ringer Zeiterfassungssysteme hat, soweit sie dazu gesetzlich verpflichtet ist, einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellt, dem die erforderliche Zeit zur Erledigung seiner Aufgaben gewährt wird. Der Datenschutzbeauftragte nimmt die Aufgaben gem. § 4g BDSG wahr.
11. Ist der KUNDE gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Daten zu geben, so wird die Ringer Zeiterfassungssysteme den KUNDEN in seinem Verantwortungsbereich darin unterstützen, diese Auskünfte zu erteilen. Soweit nicht ausdrücklich anders vereinbart, wird der Aufwand der Unterstützungsleistungen der Ringer Zeiterfassungssysteme gesondert vergütet.
12. Macht der Betroffene sein Recht auf Berichtigung, Löschung oder Sperrung seiner Daten geltend, wird die Ringer Zeiterfassungssysteme diese Anfrage an den KUNDEN weiterleiten, den KUNDEN bei der Beantwortung der Anfrage auf Anfordern unterstützen und auf Weisung des KUNDEN die Berichtigung, Sperrung oder Löschung vornehmen.

§7 Technische und organisatorische Sicherheitsmaßnahmen

1. Die Datenverarbeitung findet auf Datenverarbeitungs- Anlagen statt, für die technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten getroffen wurden. In diesem Zusammenhang wird die Ringer Zeiterfassungssysteme alle

vereinbarten Maßnahmen treffen, die für die Verarbeitung der überlassenen Daten auf den Datenverarbeitungs-Anlagen der Ringer Zeiterfassungssysteme gemäß Anlage zu § 9 BDSG für die Durchführung der Aufträge i.S.d. § 9 BDSG erforderlich sind. Näheres zu den vereinbarten technischen und organisatorischen Maßnahmen nach § 9 BDSG und Anlage zu § 9 BDSG regelt der Hauptvertrag und die Leistungsvereinbarungen.

2. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Die Maßnahmen werden erst nach entsprechender Weisung des KUNDEN ausgeführt. Der KUNDE ersetzt der Ringer Zeiterfassungssysteme den durch die Anpassung der Schutzmaßnahmen nach § 9 BDSG an den technischen Fortschritt entstehenden Mehraufwand.

§8 Datengeheimnis

Die Ringer Zeiterfassungssysteme wird das Datengeheimnis und das Fernmeldegeheimnis wahren und seine Mitarbeiter entsprechend verpflichten.

§9 Unterauftragnehmer

Die Ringer Zeiterfassungssysteme darf zur Erfüllung der nach dem Hauptvertrag zu erbringenden Leistungen nur nach vorheriger schriftlicher Zustimmung durch den KUNDEN Unterauftragnehmer einsetzen. Die Zustimmung zum Einsatz eines Unterauftragnehmers kann nur erteilt werden, wenn die Ringer Zeiterfassungssysteme Namen und Anschrift des Unterauftragnehmers mitteilt. Außerdem muss die Ringer Zeiterfassungssysteme erklären, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat. Die Ringer Zeiterfassungssysteme muss mit Subunternehmern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen dieser Vereinbarung entsprechen. Insbesondere muss der KUNDE berechtigt sein, Kontrollen vor Ort beim Subunternehmer durchzuführen oder durch Dritte durchführen zu lassen. Die Ringer Zeiterfassungssysteme hat die Einhaltung der Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten an Unterauftragnehmer ist erst zulässig, wenn der Unterauftragnehmer die Verpflichtung nach § 11 BDSG erfüllt hat. Für die in Annex 1 aufgeführten Unterauftragnehmer und die dort genannten Aufgabenbereiche gilt die Zustimmung des KUNDEN als erteilt. Der KUNDE ist zum Widerruf der Zustimmung zum Einsatz eines Subunternehmers berechtigt, wenn die Voraussetzungen nach dieser Ziffer nicht mehr vorliegen. Der Einsatz von Unterauftragnehmern durch einen Unterauftragnehmer unterliegt den gleichen Zustimmungsvoraussetzungen durch den KUNDEN, wie der in dieser Ziffer beschriebene Einsatz von Unterauftragnehmern. Der Einsatz von Unterauftragnehmern in Ländern außerhalb der EU/des EWR ist nicht gestattet.

§10 Vertragsdauer

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages.

§11 Sonstiges

1. Die Unwirksamkeit einer Bestimmung dieser Vereinbarung berührt die Gültigkeit der übrigen Bestimmungen nicht. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.
2. Änderungen dieser Vereinbarungen sowie Nebenabreden bedürfen der Schriftform. Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.
3. Es besteht zwischen den Parteien Einigkeit darüber, dass die "Allgemeinen Geschäftsbedingungen" des Auftraggebers auf diese Vereinbarung keine Anwendung finden.
4. Alleiniger Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist, vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes, Biberach/Riss.
5. Es gilt deutsches Recht.
6. Im Fall von Widersprüchen von Regelungen dieser Vereinbarung und Regelungen aus sonstigen Vereinbarungen gilt § 21 der Allgemeinen Geschäftsbedingungen für Hosting und Betrieb von ATOSS-Produkten. Im Übrigen bleiben die Regelungen des Hauptvertrags unberührt und gelten für diese Vereinbarung entsprechend.

Annex 1

Genehmigte Subunternehmen:

Annex 2

Festgelegte Maßnahmen nach § 9 BDSG bei der Ringer Zeiterfassungssysteme (hier: Auftragsdatenverarbeiter)

1. Zutrittskontrolle

Es sind keine Maßnahmen zur Zutrittskontrolle erforderlich, weil

( ) Es existieren keine Maßnahmen zur Zutrittskontrolle.
(x) Es existieren folgende Maßnahmen zur Zutrittskontrolle: Alle DV-Anlagen befinden sich in Räumen oder Rechenzentren mit Zutrittskontrolle. Der für den Zugang autorisierte Personenkreis für die Rechenzentren wird vom Auftragsdatenverarbeiter festgelegt und vor Ort durch entsprechendes Support-Personal des Rechenzentrumsbetreibers (Subunternehmer) mindestens per Sichtkontrolle authentifiziert. Der Zutritt wird protokolliert. Er erfolgt dann per elektronischem Zutrittskontrollsystem. Die Außenhaut der Rechenzentren unterliegt einer kompletten Videoüberwachung nebst Einbruch- und Kontaktmeldern. Die technischen Mitarbeiter des Subunternehmers erhalten nach denselben Regeln Zugriff zu den Rechenzentren. IT-Verantwortliche des Subunternehmers haben eine permanente Zutrittsberechtigung für die Rechenzentren. Die Zutrittskontrolle der Mitarbeiter zu den DV-Anlagen in den Arbeitsräumen des Subunternehmers erfolgt per elektronischem Zutrittskontrollsystem. Personen, die nicht zum Kreis der Mitarbeiterinnen des Auftragsdatenverarbeiters oder des Subunternehmers gehören (beispielsweise Wartungstechniker), erhalten ebenfalls nach denselben Regeln Zutritt zu den Rechenzentren.

2. Zugangskontrolle

Es sind keine Maßnahmen zur Zugangskontrolle erforderlich, weil

( ) Es existieren keine Maßnahmen zur Zugangskontrolle.

(x) Es existieren folgende Maßnahmen zur Zugangskontrolle: Zugänge zu den DV-Anlagen sind grundsätzlich personenbezogen passwortgeschützt, wobei die Passwörter in Zyklen geändert werden müssen. Die Änderung und die damit verbundenen Änderungsregelungen von Passwörtern obliegt dem Auftragsdatenverarbeiter. Die Passwortregelungen entsprechen den Anforderungen, die zu einer ISO 27001 ff. notwendig sind. Grundsätzlich liegt die Verantwortlichkeit für die vollen Administrationsprivilegien (Zuweisung von Passwörtern und Änderungsregelungen) und für die Zugangskontrolle beim Auftragsdatenverarbeiter. In Notfällen kann die jeweilige, nicht personifizierte Systemadministratorenkennung verwendet werden. Diese wird unter Verschluss vom Auftragsdatenverarbeiter verwaltet und in regelmäßigen Abständen geändert. Die Verwendungsprotokolle sind durch den Auftragsdatenverarbeiter jederzeit einsehbar und abrufbar.

3. Zugriffskontrolle

Es sind keine Maßnahmen zur Zugriffskontrolle erforderlich, weil

( ) Es existieren keine Maßnahmen zur Zugriffskontrolle.

(x) Es existieren folgende Maßnahmen zur Zugriffskontrolle: Das Berechtigungskonzept umfasst sämtliche Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern, die Einschränkung der Zugriffsmöglichkeit des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten (z.B. funktionale Zuordnung einzelner Datenendgeräte; automatische Prüfung der Zugriffsberechtigung; differenzierte Zugriffsberechtigung auf Dateien, Datensätze, Datenfelder, Anwendungsprogramme, Betriebssysteme und differenzierte Verarbeitungsmöglichkeiten wie Lesen, Ändern, Löschen).

4. Weitergabekontrolle

Es sind keine Maßnahmen zur Weitergabekontrolle erforderlich, weil

( ) Es existieren keine Maßnahmen zur Weitergabekontrolle.

(x) Es existieren folgende Maßnahmen zur Weitergabekontrolle: Die Weitergabekontrolle umfasst die Regeln zur Weitergabe von Datenträgern, die Nutzung von privaten Datenträgern, die Mitnahme von Behältnissen in Räume mit DV-Anlagen, die Vernichtung von Datenträgern. Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung sowie beim Transport von Datenträgern wird dadurch verhindert, dass Zugang und Datenverarbeitung grundsätzlich über verschlüsselte Verbindungen, beispielsweise über SSH, HTTPS oder RDP erfolgen. Bei Koppelungen von internen Netzen wird eine VPN-Kopplung eingesetzt. Wo der Zugang aus technischen Gründen nicht über eine verschlüsselte Verbindung möglich ist (z.B. Telnet- oder VNC-Zugänge), existieren andere Mechanismen (VLAN, MPLS, Firewallschaltungen) zur Eingrenzung auf den für die Entstörung erforderlichen Personenkreis. An welcher Stelle Datenübermittlung durch Einrichtungen zur Datenübertragung vorgesehen ist, kann durch die Dokumentation der vorgesehenen Abruf- und Übermittlungsvorgänge bzw. Dokumentation der Übermittlungsstellen und –wege überprüft und festgestellt werden.

5. Eingabekontrolle

Es sind keine Maßnahmen zur Eingabekontrolle erforderlich, weil

( ) Es existieren keine Maßnahmen zur Eingabekontrolle.

(x) Es existieren folgende Maßnahmen zur Eingabekontrolle: Ob und von wem Daten in DV-Systemen eingegeben, verändert oder entfernt worden sind, kann grundsätzlich überprüft und festgestellt werden anhand des Zugangs, der in den Systemprotokollen dokumentiert wird. Dabei wird, mindestens ohne weitere Sicherungsmaßnahmen, auf dem jeweiligen System folgendes gespeichert: Die persönliche Kennung und der Zugangszeitpunkt für den Zeitraum von einem Monat. Bei besonderen Anforderungen werden diese Daten zentral gespeichert und die Vorhaltezeit verlängert. Bei besonderen Anforderungen wird die Vorbereitung von Datenänderungen, die

Freigabe und deren Einspielung auf getrennte, jeweils dafür verantwortliche Personenkreise beschränkt. Weitere Maßnahmen wie Erfassungsbelege mit Erfassungs- und Prüfbestätigung, Protokollierung eingegebener Daten, Verarbeitungsprotokolle u.a. können nach spezieller Beauftragung durch den KUNDEN gegen Entgelt eingeführt und entsprechend dokumentiert werden.

6. Auftragskontrolle

Es sind keine Maßnahmen zur Auftragskontrolle erforderlich, weil hierfür nur der KUNDE verantwortlich ist.

( ) Es existieren keine Maßnahmen zur Auftragskontrolle.

(x) Es existieren folgende Maßnahmen zur Auftragskontrolle:

a.) die Subunternehmer wurden sorgfältig ausgewählt

b.) die Subunternehmer wurden verpflichtet, ihre Mitarbeiter auf das Datengeheimnis zu verpflichten

c.) der KUNDE wurde schriftlich über den Einsatz der Subunternehmer informiert

d.) es liegt ein schriftlicher Vertrag zwischen dem Auftragsdatenverarbeiter und den Subunternehmern (mittelbar mit deren Subunternehmern) gem. § 11 BDSG vor □ eine Auftrags-, Weisungsbefugnis ist schriftlich geregelt,

e.) die Einhaltung der technischen und organisatorischen Maßnahmen beim Subunternehmer wird regelmäßig kontrolliert.

7. Verfügbarkeitskontrolle

Es sind keine Maßnahmen zur Verfügbarkeitskontrolle erforderlich, weil

( ) Es existieren keine Maßnahmen zur Verfügbarkeitskontrolle.

(x) Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle: Die Rechenzentren verfügen über eine unterbrechungsfreie Versorgung (Strom und Klimatisierung). Je nach Beauftragung werden für Katastrophenfälle auch die Systeme vollständig redundant an getrennten Standorten bereitgehalten, bzw. werden die Daten der Kundensysteme mit entsprechenden Sicherungs- oder Speichersystemen an getrennten Standorten gespeichert. Für Server existieren grundsätzlich Back-ups, üblicherweise ein tägliches Voll-Back-up. Tatsächliche Vorhaltezeit und tatsächlicher Rhythmus können je nach Beauftragung, dem jeweiligen System und Datenbestand angemessen variieren. Die Daten werden vollständig automatisiert und, über ein Storagesystem gepuffert, auf Magnetband geschrieben. Grundsätzlich werden dem technischen Stand entsprechend und den Anforderungen angemessene, regelmäßig aktualisierte Firewallsysteme und Antivirenschutzsysteme eingesetzt.

8. Verwendungszweckkontrolle

Es sind keine Maßnahmen zur Verwendungszweckkontrolle erforderlich, weil

( ) Es existieren keine Maßnahmen zur Verwendungszweckkontrolle.

(x) Es existieren folgende Maßnahmen zur Verwendungszweckkontrolle: Vom Auftragsdatenverarbeiter wird die getrennte Bereitstellung der Systeme gewährleistet.