Vereinbarung zur Auftragsverarbeitung

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

Atoria

Präambel

Diese Vereinbarung zur Auftragsverarbeitung spiegelt die Vereinbarung der Parteien in Bezug auf die Bedingungen wider, die die Verarbeitung der personenbezogenen Daten des Kunden (nachfolgend „Auftraggeber" genannt) durch die Atoria – the people software GmbH (nachfolgend „Auftragnehmer" genannt) unter den zwischen den Parteien bestehenden Vertragsverhältnisses regeln. Die Vereinbarung zur Auftragsverarbeitung wird durch Bezugnahme in jeweiligen Vertragsdokumenten zwischen den Parteien rechtswirksam als Anlage in die zwischen den Parteien bestehenden Vertragsverhältnis aufgenommen.

Für Bestandskunden gilt, dass durch das Bereitstellen dieser Vereinbarung vom Auftragnehmer an den Auftraggeber das zwischen den Parteien bestehende Vertragsverhältnis rechtswirksam ergänzt und somit zwischen den Parteien rechtsverbindlich vereinbart wird.

Der Auftraggeber hat den Auftragnehmer mit der Bereitstellung von Services aus dem Produkt- und Serviceportfolio der Atoria – the people software GmbH beauftragt. In diesem Zuge verarbeitet der Auftragnehmer auch personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers.

Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1 Gegenstand des Auftrags, Art und Zweck der Verarbeitung

1) Beratung, Implementierung, Betreuung, Support, Wartung und Präsentationen der HR, MES und Security Software mit allen Modulen sowie das erweiterte Softwareangebot, das durch Atoria vertrieben und implementiert wird. Der Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich im Weiteren aus **Anlage 1**.

(2) Im Übrigen ergibt sich der Gegenstand des Auftrags aus dem Hauptvertrag und den Folgeaufträgen und auf die hier verwiesen wird (im Folgenden „Hauptvertrag").

2 Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Art der Daten:

Die Art der personenbezogenen Daten ergibt sich aus **Anlage 1**.

(2) Kreis der betroffenen Personen:

Der Kreis der betroffenen Personen ergibt sich aus **Anlage 1**.

3 Dauer des Auftrages

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

4 Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

(3) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5 Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

6 Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

Dabei sind 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 im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(2) Die Vertragsparteien vereinbaren die in dem **Anlage 3** zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber über das Trustcenter mitzuteilen.

7 Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer erteilt dem Auftraggeber hiermit die allgemeine Genehmigung zur Hinzuziehung von Subunternehmern: *Die Liste der Subunternehmer befindet sich unter* ***Anlage 2***. Über den geplanten Einsatz eines weiteren Subunternehmers oder den Austausch eines bestehenden Subunternehmers hat der Auftragnehmer den Auftraggeber rechtzeitig vorab über das Trustcenter zu informieren. Die Zustimmung zur Untervergabe gilt als erteilt, wenn der Auftraggeber nicht innerhalb von 6 (sechs) Wochen, beginnend mit Zugang der Information in vorstehendem Sinne, dem Einsatz des betreffenden Subunternehmers widerspricht. Ein solcher Widerspruch ist nur aus berechtigten Gründen zulässig, wie z. B. nicht ausreichende Zuverlässigkeit des Subunternehmers.

Widerspricht der Auftraggeber dem Einsatz eines vom Auftragnehmer gewünschten Subunternehmers, so ist der Auftragnehmer berechtigt, den Hauptvertrag ohne Einhaltung einer Kündigungsfrist und mit sofortiger Wirkung zu kündigen.

(3) Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Die Verarbeitung der Daten durch den Auftragsverarbeiter und die vom Verantwortlichen genehmigten Subdienstleister findet grundsätzlich in Mitgliedstaaten der Europäischen Union, Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und/oder solchen Ländern statt, für die ein gültiger, auf die Verarbeitung anwendbarer Angemessenheitsbeschluss der Kommission im Sinne des Art. 45 Abs. 3 DSGVO vorliegt. Es ist dem Auftragsverarbeiter gestattet,

Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb der EU/ des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und sicherstellt, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Die Regelung aus 7 (2) dieser Vereinbarung gilt somit auch für die Beauftragung von Subdienstleistern im Drittstaat.

(6) Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subunternehmer aufzuerlegen.

8 Unterstützung bei der Wahrung von Betroffenenrechten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(2) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g DSGVO). Auskünfte an Dritte oder den betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(3) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9 Unterstützung bei Dokumentations- und Meldepflichten

(1) Ist der Auftragnehmer nach Art. 37 DSGVO, § 38 BDSG gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten zu benennen, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten auf Anfrage zum Zweck der direkten Kontaktaufnahme mit.

(2) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO. Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

(3) Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

(5) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

10 Beendigung des Auftrages

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

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

11 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens 72 Zeitstunden, werktäglich) durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden machen. Sollte der durch den Auftraggeber beauftragte Prüfer

in einem direkten Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist diejenigen Auskünfte zu erteilen, die zum Nachweis der Einhaltung der Pflichten unter diesem Auftragsverarbeitungsvertrag sowie zum Nachweis der technischen und organisatorischen Maßnahmen erforderlich sind. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit vorlegen. Der Auftraggeber hat dem Auftragnehmer den durch die Erteilung der Auskünfte entstehenden Aufwand zu vergüten.

12 Haftung

Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz, oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

13 Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

(3) Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(4) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 1: Angaben zur Datenverarbeitung
- Anlage 2: Genehmigte Subunternehmer
- Anlage 3: Technische und organisatorische Maßnahmen Atoria
- Anlage 4: Bei Nutzung der My Business Cloud Hosting / SaaS, TOM-Rechenzentrum
- Anlage 5: Datenschutzrelevante Punkte bei Nutzung der tisoware.APP

Anlage 1

Angaben zur Datenverarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

Der Auftragnehmer erbringt für den Auftraggeber unterschiedliche Dienstleistungen aus dem Produkt- und Serviceportfolio der Atoria in der Funktion eines Generalunternehmers. Diese Anlage 1 enthält die auftragsspezifischen Leistungen und Datenverarbeitung i.S.d. Art. 28 Abs. 3 S. 1 DSGVO für die jeweils vom Auftragnehmer erbrachten Services.
Die für diese Vereinbarung geltenden Angaben richten sich stets nach den konkreten Services, die Inhalt des zwischen den Parteien geschlossenen Hauptvertrags sowie ergänzender Vereinbarungen sind.

tisoware HR, MES und Security-Module

Der Auftragnehmer installiert, implementiert und wartet Softwaresysteme aus der Produktpalette der Atoria – the people software GmbH für den Auftraggeber und erbringt Werk- und/oder Dienstleistungen gemäß Vertragsvereinbarung des bestehenden Hauptvertrags. Diese Wartungsarbeiten und Dienstleistungen können vor Ort beim Auftraggeber oder mittels Fernwartung und Kundenbetreuung durch den Auftragnehmer erfolgen. Ein Zugriff auf personenbezogene Daten des Auftraggebers kann hierbei nicht ausgeschlossen werden.

Gegenstand der Verarbeitung	**Art der Daten**	**Kreis der Betroffenen**	**Zweck**
Zugriff auf Kundensysteme vor Ort oder per Fernwartung im Rahmen des Einsatzes von tisoware.MODULEN der Atoria	Personenstammdaten (z.B. Name, Vorname, Personalnummer) Zeiterfassungsdaten (z.B. Kommen-, Gehen-, Pausenzeiten) Personaleinsatzplanungsdaten (z.B. Schichten, Schichtmodelle, Urlaubsanträge, Abwesenheiten) Personendaten in Verbindung mit Betriebs- und Maschinendaten (Auftragsbeginn, Details zur Auftragsdurchführung) Kantinendaten in Verbindung mit Personendaten (Konsumation) Zutrittsdaten (z.B. Name, Vorname, Zutrittszeit/-ort) Besucherdaten (z.B. Name, Vorname, Firma, Besuchszeiten) Reisedaten in Verbindung mit Personendaten	Beschäftigte des Auftraggebers Besucher	Beratung, Schulung, Software-Installation und -Wartung, Update-Installation, Support (inkl. Fernwartung), Reorganisation der Datenbank

Bei On-Prem Installationen

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung, insbesondere hinsichtlich der Erteilung von Auskünften und die Erfüllung von Löschungsersuchen, allein verantwortlich. Der Auftragnehmer verpflichtet sich seinerseits, die Vorschriften der DS-GVO und sonstiger Datenschutzvorschriften einzuhalten.

Zusatz bei Modul: tisoware.eAU (elektronische Arbeitsunfähigkeitsbescheinigung)

Die eAU-Daten werden mitarbeiterbezogen automatisch bei der GKV angefragt. Der Arbeitgeber wird durch entsprechende Rückmeldungen über Beginn und Dauer einer Arbeitsunfähigkeit informiert.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Zugriff auf Kundensysteme vor Ort oder per Fernwartung im Rahmen des Einsatzes der Software	Daten der elektronischen Arbeitsunfähigkeitsbescheinigung (z.B. AU-Beginn, AU-Ende, Erst/Folgebescheinigung, SV-Nummer, Betriebsnummer AG/KK, Arbeitsunfall) Daten aus Lohnprogramm (Personalnummer, Eintritts-Austrittsdatum SV, SV-Nummer, Geburtsdatum,-Name,-Ort)	Alle Betroffenen, deren Daten im Rahmen der Atoria.Applikationen durch den Auftraggeber verarbeitet werden	Automatische, mitarbeiterbezogene Abfrage der elektronischen Arbeitsunfähigkeitsbescheinigung beim Server der GKV über Beginn und Dauer einer Arbeitsunfähigkeitsbescheinigung über eine von der ITSG zertifizierten Schnittstelle.

My Business Cloud Hosting / SaaS

Leistungsgegenstand des Auftragnehmers ist die Bereitstellung und Betrieb von IT-Systemressourcen (Server-Hosting), einschließlich Hardware, Speicherplatz und der dafür erforderlichen Betriebssysteme sowie Erbringung bestimmter Installations-, Administrations- und sonstiger Dienstleistungen, die insgesamt den Fernzugriff des Kunden auf die Vertragssoftware über Internetverbindung in einer dedizierten, kundenspezifischen virtuellen Umgebung zu ermöglichen, mit dem Zweck, eine klassische on-prem Installation beim

Kunden zu ersetzen. Auf den Umfang und die Art der durch den Auftraggeber bearbeiteten Daten hat der Auftragnehmer keinen Einfluss.

Gegenstand der Verarbeitung	Art der Daten	Kreis der Betroffenen	Zweck
Bereitstellung von Servern für den externen Betrieb der My Business Cloud Hosting / SaaS	Alle Daten, die im Rahmen der Atoria.Applikationen durch den Auftraggeber verarbeitet werden	Alle Betroffenen, deren Daten im Rahmen der Atoria.Applikationen durch den Auftraggeber verarbeitet werden	Betrieb der My Business Cloud auf Servern des Auftragnehmers

Reutlingen, 21.01.2025

Anlage 2

Genehmigte Subunternehmer

Atoria erklärt, dass die nachfolgenden Subunternehmer eingesetzt werden:

Subunternehmer	Verarbeitungstätigkeit	Ort der Datenverarbeitung	Geeignete Garantien, Art. 44 ff. DSGVO (falls erforderlich)	Zusätzliche Maßnahmen zum Schutz personenbezogener Daten (falls erforderlich)
dormakaba Deutschland GmbH, Access Solutions DACH DORMA Platz 1 58256 Ennepetal	Lieferung von Hardware aus der Produktpalette des Lieferanten, Eventuelle Installations- und Entstörungsmaßnahmen	EU	-	-
PCS Systemtechnik GmbH Pfälzer-Wald-Str. 36 81539 München	Lieferung von Hardware aus der Produktpalette des Lieferanten, Eventuelle Installations- und Entstörungsmaßnahmen	EU	-	-
Datafox GmbH Dermbacher Straße 12-14 36419 Geisa	Lieferung von Hardware aus der Produktpalette des Lieferanten, Eventuelle Installations- und Entstörungsmaßnahmen	EU	-	-
FORSIS GmbH Schwabenstraße 5 88214 Ravensburg	Lieferung von Hardware aus der Produktpalette des Lieferanten, Eventuelle Installations- und Entstörungsmaßnahmen	EU	-	-
IDENTA Ausweissysteme GmbH Steinkirchring 16 78056 Villingen-Schwenningen	Herstellung von Ausweismedien	EU	-	-
MADA Marx Datentechnik GmbH Hinterhofen 4 78052 Villingen-Schwenningen	Herstellung von Ausweismedien	EU	-	-

Subunternehmer	Verarbeitungstätigkeit	Ort der Datenverarbeitung	Geeignete Garantien, Art. 44 ff. DSGVO (falls erforderlich)	Zusätzliche Maßnahmen zum Schutz personenbezogener Daten (falls erforderlich)
ACP IT Solutions AG Carl-Jordan-Str. 18a 83059 Kolbermorr	Bereitstellung cloud-basierter Dienst: Infrastructure as a Service bei Cloud Kunden	EU	-	-
Quick-Lohn Software GmbH Wiesenstr. 32 16230 Britz	Bereitstellung cloud-basierter Dienst: bei eAU Kunden	EU	-	-
ICARO Software GmbH Industriestrasse 27 E 63834 Sulzbach am Main	Lieferung von Software aus der Produktpalette des Lieferanten, Installations-, und Störungsbeseitigung bei Kunden des Auftraggebers vor Ort oder durch Fernwartungszugriff	EU	-	-
proALPHA Group GmbH Auf dem Immel 8 67685 Weilerbach	Zur Verfügungstellung von Shared Services im Bereich internes IT-Management/ Services	EU	-	-

Anlage 3

Technische und organisatorische Maßnahmen

Atoria verfolgt ein übergreifendes Standortsicherheitskonzept. Dieses ist, mit Ausnahme einer standortspezifischen Zutrittskontrolle, hinsichtlich der weiteren TOM übergreifend verbindlich definiert.

In der hier vorliegenden Beschreibung über den aktuellen Stand der grundlegenden Maßnahmen zum Schutz der Daten wird einschränkend darauf hingewiesen, dass verständlicherweise nicht alle Sicherheitsmaßnahmen im Detail offengelegt werden können. Gerade in Bezug auf Datenschutz und Datensicherheit ist der Verzicht auf vertrauliche und detaillierte Beschreibungen unabdingbar, da der Schutz der Sicherheitsmaßnahmen gegen unbefugte Offenlegung mindestens genauso wichtig ist wie die Sicherheitsmaßnahmen selbst.

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

- Einsatz der elektronischen Zutrittssicherung tisoware.ZUTRITT zur Sicherung der Geschäftsräume in Verbindung mit RFID-Ausweisen
- Protokollierung der Zutritte in der elektronischen Zutrittssicherung tisoware.ZUTRITT
- Mehrstufiges Rechtekonzept: Mitarbeiter erhalten Zutrittsrechte individuell nach Funktionsbereich
- Absicherung bestimmter Büroräume durch zusätzliche Zutrittsleser, Fingerprint- oder Handvenen-Lesern. Zutrittsrechte für diese Büroräume werden bestimmten Mitarbeitern individuell nach Funktionsbereich in der elektronischen Zutrittssicherung tisoware.ZUTRITT vergeben.
- Absicherung der IT-System-Räume, Serverräume durch den Einsatz von Fingerprint- und Handvenen-Lesern
- Schnellstmögliche Sperrung der RFID-Ausweise bei etwaigem Verlust
- Absicherung des Hauptgebäudes über zusätzliche mechanische Schließanlage sowie Handvenen-Leser.
- Dokumentierte Ausgabe von RFID-Ausweisen und Schlüsseln ausschließlich an Mitarbeiter
- Videoüberwachung im Eingangsbereich des Hauptgebäudes sowie von bestimmten Teilbereichen (IT) in den Geschäftsräumen des Auftragsnehmers
- Alarmsicherung des kompletten Bürogebäudes und Überwachung durch Sicherheitsdienst
- Besucher und Dienstleister dürfen nur in Begleitung von berechtigten Mitarbeitern die Geschäftsräume und Sicherheitsbereiche betreten.
- das Reinigungspersonal ist bei Atoria fest angestellt
- in Ausnahmefällen kann es erforderlich sein, die Fernwartung (über geeignete Softwaretools) durch den zuständigen Mitarbeiter auch im Home-Office ausführen zu lassen. Der Mitarbeiter

führt diese Fernwartung auf einem Atoria eigenen Rechner durch. Der Atoria Rechner ist Passwort geschützt und verschlüsselt.

- Rechenzentren mit Standort in Deutschland oder der EU

Rechenzentren zertifiziert nach ISO 27001

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.

- Absicherung der DV-System-Räume durch den Einsatz von Leser/Scanner
- Userbezogenes ADS-Passwort mit zyklischer Neuvergabe
- Externer Zugang nur über gesicherte und verschlüsselte VPN-Verbindungen
- Getrenntes Gäste-WLAN
- Detaillierte Benutzerprofile
- Authentifikation mit Benutzer + Passwort
- Passwortregelungen
  - Verwendung von individuellen Passwörtern
  - Passwörter mit einer Mindestlänge
  - Anzahl von aufeinanderfolgenden Fehlversuchen ist begrenzt
  - Passworthistorie
- Verschlüsselung von mobilen Datenträgern
- Autonome Fernwartung
- Bestandteil des Sicherheitskonzeptes der pA Gruppe
- Zentrale Änderung der Zugangsberechtigungen durch IT-Verantwortliche
- Protokollierung der Serverzugriffe auf Benutzerebene

Zugriffskontrolle

Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass bei Erfüllung der Aufgaben nach § 1 solche Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

- Detailliertes Berechtigungskonzepts
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste" reduzieren
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (i.d.R. Möglichkeit mit Zertifikat)
- Einsatz von Intrusion-Detection-Systemen
- Differenzierte Zugriffsberechtigungen auf Dateien, Datensätze, Datenfelder und Anwendungsprogramme

- Protokollierung der Zugriffe (Datenbanken, File- und Kundensysteme)
- Bereiche mit personenbezogenen Daten sind auf externen Medien durch bestimmte Software verschlüsselt
- Einsatz von VPN-Technologie
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Einsatz von Anti-Viren-Software

Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Festlegung von Datenbankrechten
- Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten
- anderer Kunden Rechnung trägt
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)

2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Maßnahmen, die sicherstellen, 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.

- Elektronische Übertragung, Datentransport, sowie deren Kontrolle.
- Einsatz von verschlüsselten Verbindungen (z.B. VPN, HHPS)
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- Shredder für die sichere Vernichtung von Daten
- Datenschutzboxen für die Entsorgung von vertraulichen Papierdokumenten über eine spezialisierte Entsorgungsfirma

Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Folgende Aktivitäten werden protokolliert: Hoch- und Herunterfahren von zentralen Rechnern (v.a. Servern und Firewalls)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Datenpflege nur durch Atoria Mitarbeiter

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle und Belastbarkeit

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

- Brandschutzmaßnahmen durch den Vermieter des Gebäudes vorgenommen:
  - Rauchmelder installiert in allen Fluren - Alarme aufgeschaltet bei der Feuerwehr
  - Feuer-Einrichtung mit Wandhydrant installiert in allen Fluren
- ausreichend Feuerlöscher installiert, Feuerlöscher mit CO2 vor den Serverräumen
- Klimaanlage in Serverräumen installiert
- Feuerlöschgeräte in Serverräumen
- Testen von Datenwiederherstellung
- Schutzsteckdosenleisten in Serverräumen
- Serverräume nicht unter sanitären Anlagen
- Backup- & Recoverykonzept
- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung von Datensicherung an einem sicheren, separaten Ort
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen / IT-Räumen

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Kontrollverfahren

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.

- Unternehmensrichtlinien (Code of Conduct) vorhanden
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Datenschutz-Management vorhanden
- Datenschutz-Konzept vorhanden

5 Technische und Organisatorische Maßnahmen im Home Office

Atoria ermöglicht den Mitarbeitern, anfallende Arbeiten via Remote-Zugang durchzuführen. Hierfür wurden Maßnahmen ergriffen, um dem Sicherheitsstandard des allgemeinen Sicherheitskonzeptes zu entsprechen. Dieses gilt, soweit anwendbar und wird um die folgenden Maßnahmen ergänzt.

Die Maßnahmen unterteilen sich in **technische Maßnahmen**, die den Zugang zum System betreffen sowie in **organisatorische Maßnahmen**, die den Umgang des jeweiligen Mitarbeiters mit Daten an seinem Heimarbeitsplatz betreffen.

Technische Maßnahmen

Die nachfolgenden Maßnahmen stellen die zusätzlich ergriffenen Maßnahmen dar. Für den Zugriff auf das System hat Atoria folgende Maßnahmen getroffen:

- Zugang ausschließlich über dienstliche Endgeräte
- Endgeräte werden IT-seitig regelmäßigen Updates unterzogen
- Applikationen dürfen ausschließlich nach Konsultation der hierfür vorliegenden Whitelist installiert werden. IT-seitig nicht zugelassene Applikationen dürfen nicht installiert werden
- Ein Zugriff erfolgt ausschließlich durch eine verschlüsselte VPN-Verbindung
- Windows Clients
  - Endpoint Security
  - Antivirus Software
  - Systemverschlüsselung
  - Proxy zur Domainfilterung
- iOS Clients
  - verwaltet durch Airwatch MDM/Workspace One
    - Kontrolle über das Gerät mit Möglichkeit zum remote „wipe“ bzw. „lock“
  - komplette Verschlüsselung des Gerätes
  - geschützt durch sechsstelligen Pass Code
  - restriction policy
    - nicht vertrauenswürdige Zertifikate können nicht manuell akzeptiert werden
    - keine Diagnosedaten an Apple
    - Benutzer kann keinen 3rd-Party Apps manuell vertrauen

Organisatorische Maßnahmen

In organisatorischer Hinsicht wurden in Ergänzung zu den Maßnahmen der allgemeinen TOM verschiedene Zusatzvereinbarungen sowie interne Richtlinien erlassen. Dies umfasst unter anderem Folgende Regelungen und Verpflichtungen:

- Zutritts- und Kontrollrecht des Arbeitsplatzes durch interne beauftragte Prüfer (z.B. Fachkraft für Arbeitssicherheit oder betrieblicher Datenschutzbeauftragter)
- Verpflichtung auf interne Richtlinie zur Nutzung technischer Einrichtungen
- Verpflichtung zum Schutz des Zugriffs unbefugter Dritter auf Arbeitsmittel

- Untersagung der Verwendung eigener technischer Einrichtungen (Ausgenommen WLAN, Peripheriegeräten wie Tastatur und Maus ohne Treiberinstallation)
- Verpflichtung, vertrauliche dienstliche Dokumente unter Verschluss zu halten
- Verpflichtung auf Vertraulichkeit / zur Geheimhaltung

Verpflichtung, Wohnortswechsel mitzuteilen

Anlage 4

Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO“ (TOM) bei ACP IT Solutions AG (Rechenzentrum) als Partner für Atoria-Kundenprojekte, Stand: 07.08.2019

ACP IT Solutions AG (im weiteren ACP genannt) stellt Leistungen für Atoria bzw. deren Projektkunden bereit und hat insbesondere die folgenden Maßnahmen nach Art. 32 DSGVO ergriffen:

1. Allgemeine Maßnahmen, Organisation von Datenschutz und Informationssicherheit

- **IS27001-Zertifizierung**. ACP ist nach ISO27001 zertifiziert. Die Zertifizierung umfasst die Organisationseinheiten Rechenzentrumsbetrieb (ACP Cloud Server), Managed Services, Service Desk und Service Operations (ACP Services).

- **Risikobewertung**. Eine Risikoanalyse und Risikobewertung in Hinblick auf die Schutzziele der Vertraulichkeit, Verfügbarkeit und Integrität der Kundendaten ist im Rahmen der ISO27001- Zertifizierung erfolgt. Da ACP als Auftragsverarbeiter tätig ist, erfolgt keine Analyse der spezifischen Risiken der Datenverarbeitungsvorgänge, die der Kunde mit den von ACP bereitgestellten oder gewarteten Systemen durchführt, da der Kunde insoweit selbst Verantwortlicher ist.

- **Rollen für Sicherheit und Datenschutz**. ACP hat einen Informationssicherheits-beauftragten und einen Datenschutzbeauftragten bestimmt.

- **Geheimhaltungsverpflichtung**. Mitarbeiter von ACP unterliegen Geheimhaltungs-verpflichtungen und sind auf das Datengeheimnis belehrt.

- **Richtlinien und Arbeitsanweisungen**. ACP führt Richtlinien und Sicherheits-dokumentation, in denen die Sicherheitsmaßnahmen und die relevanten Verfahren und Verantwortlichkeiten ihrer Mitarbeiter beschrieben sind.

- **Sicherheits- und Datenschutz-Schulungen**. ACP informiert ihre Mitarbeiter über relevante Datenschutz- und Sicherheitsmaßnahmen und ihre jeweiligen Aufgaben. Außerdem informiert ACP ihre Mitarbeiter über mögliche Konsequenzen beim Verstoß gegen die Sicherheitsvorschriften und -verfahren.

- **Auftragskontrolle** durch Abschluss von Verträgen nach Art. 28 DSGVO mit Auftragnehmern und Subunternehmern, Einräumung von Kontrollrechten und Weisungsbefugnissen, Dokumentation von Verfahren und Prozessen, Stichprobenprüfungen.

2. Besondere Maßnahmen zum Schutz von Vertraulichkeit, Verfügbarkeit und Integrität

ACP hat insbesondere die folgenden Maßnahmen getroffen, um Vertraulichkeit, Verfügbarkeit und Integrität der Kundendaten angemessen zu schützen:

Physische Sicherheit

Es soll verhindert werden, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen Kundendaten verarbeitet werden. Zu den umgesetzten Maßnahmen zählen insbesondere:

Rechenzentrum

Der Zutritt zum Rechenzentrum ist über eine 3 Faktor Authentifizierung abgesichert. Für den Zutritt wird ein physischer Token mit PIN und biometrische Merkmale benötigt.

Sowohl für den Zutritt zu einzelnen Datensicherheitsräumen als auch für das Öffnen von Schränken wird jeweils der Token benötigt.

Videoüberwachung: Der Innen- und Außenbereich ist mit Videotechnik ausgestattet (Überwachung). Die Videoaufzeichnungen werden für 90 Tage vorgehalten.

Protokollierung der Schließvorgänge: Alle Schließvorgänge der Türen beim Zutritt zum Rechenzentrum und von Datensicherungsräumen werden elektronisch erfasst und sind für Mitarbeiter des Rechenzentrums-Betreibers online einsehbar. Die Schließvorgänge der Schranktüren werden in den jeweiligen Schlössern elektronisch erfasst und sind manuell direkt an den Schlössern auslesbar.

Sicherheitsdienst: Das Rechenzentrum wird von einem Sicherheitsdienst überwacht, der mehrmals täglich sporadisch das Gebäude begeht.

Büroräume

Zutritts-Token zu den Räumlichkeiten der Service-Teams werden protokolliert vergeben. Die Räume sind in einem getrennten Zutrittsbereich nur über Zutritts-Token zugänglich. Es dürfen keine unberechtigten und unbeaufsichtigten Personen Zutritt erhalten.

Es sind zwei Systeme eingerichtet, die den Zutritt und das Verlassen des Gebäudes und somit aller Büroräume regeln:

- Schließanlage zur zentralen Verwaltung von Transpondern und Schlössern
- Einbruchmeldeanlage zur Überwachung des Objekts mit Anschluss an eine Notrufzentrale

Zugangs- und Zugriffskontrolle

Sowohl der Zutritt als auch der Zugang und Zugriff zu Systemen, in denen personenbezogene Daten verarbeitet werden, ist durch ein **Berechtigungskonzept** geschützt. ACP beschränkt den Zugang zu Systemen, in denen Kundendaten verarbeitet werden, auf autorisierte Personen. Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur erlaubt, wenn dies erforderlich ist. Generell ist der Zugriff auf Kundendaten nur auf die Personen beschränkt, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen **(„need-to-know"-Prinzip)**. Insbesondere gilt:

- Pro Benutzer existiert ein entsprechendes Benutzerkonto.
- Benutzerkennung mit Passwort (Einstellung der Passwortregeln in einer allgemein gültigen Policy)
- Zugang zu Rechnern/Systemen (Authentifizierung) durch Benutzerkennung mit Passwort
- Firewall
- 2-Faktor-Authentifizierung

Protokollierung

ACP protokolliert unter anderem

- sicherheitsrelevante Ereignisse (z.B. Firewall-Logs) und
- den Zugriff und die Nutzung auf Kundensysteme auf Basis der eindeutigen Benutzerkennungen (s.o.)
- Es wird sichergestellt, dass Protokolldaten nicht nachträglich verändert werden können.

Verschlüsselung

ACP verschlüsselt Daten bei der Übertragung im Netzwerk (SSL) und beim Transport von Datenträgern nach Branchenstandards (z.B. AES256).

Datenträgerverwaltung und Inventarisierung

ACP führt Unterlagen über die Systeme und Medien, die Kundendaten enthalten.

Datenlöschung und Datenträgerentsorgung

ACP verwendet Verfahren nach Branchenstandards, um Kundendaten und Datenträger, die Kundendaten enthalten, fachgerecht zu löschen. Nicht mehr benötigte und zu entsorgende Festplatten und Datenträger werden einer zertifizierten Entsorgung zugeführt.

Netzwerk- und Systemsicherheit

ACP setzt Maßnahmen zur Sicherung der Netzwerke, Systeme und Datenverarbeitungsgeräte vor unbefugtem Zugriff um, z.B. durch

- Verwendung von VPNs und Firewalls
- Segmentierung von Netzen und Bereitstellung von DMZ
- Verwendung gesicherter Schnittstellen (USB, Netzwerk, API, etc.)
- Umsetzung von Antivirusmaßnahmen, um zu verhindern, dass Viren oder Malware unbefugten Zugriff auf Kundendaten erhalten

Backup und Datensicherung

ACP hat Backup-Konzepte zur regelmäßigen Sicherung von Kundendaten implementiert.

Zur Datensicherung der ACP Cloud Server wird ein Datensicherungsverfahren verwendet, bei dem der gesamte Server als Image gesichert wird. Es wird dazu keine Netzwerkverbindung zwischen Datensicherungssystem und ACP Cloud Server oder administrative Accounts in den zu sichernden ACP Cloud Servern benötigt. Dadurch kann eine hohe Sicherheit bei der Durchführung der Datensicherung gewährleistet werden. Die Datensicherungen werden für jeden Werktag (6x pro Woche) durchgeführt.

Die Vorhaltezeit der gesicherten Daten kann aus 3 Service-Levels gewählt werden:

- Basic: Vorhaltezeit der Datensicherung 7 Tage
- Standard: Vorhaltezeit der Datensicherung 14 Tage
- Premium: Vorhaltezeit der Datensicherung 30 Tage

Die Datensicherung wird im Rahmen von täglichen Checklisten stichprobenartig auf Erfolg überprüft. Nicht erfolgreiche Datensicherungen werden entsprechend wiederholt. Das Ergebnis der täglichen Überprüfung wird in einem Protokoll dokumentiert.

Die Funktionsfähigkeit der Datensicherung wird monatlich anhand von Wiederherstellungstests geprüft. Das Ergebnis dieser Tests wird in einem Protokoll dokumentiert.

Für Wiederherstellungen können folgende Verfahren gewählt werden:

- Komplette ACP Cloud Server

- Einzelne virtuelle Festplatten eines ACP Cloud Servers
- Einzelne Ordner und Dateien eines ACP Cloud Servers

Mit der Option Bandzusendung wird einmal pro Monat eine vollständige Datensicherung auf LTO-Band zugesendet. Auf den Sicherungsbändern sind ACP Cloud Server als Images abgelegt. Die Bänder werden mit AES256 verschlüsselt um eine hohe Sicherheit bei der Versendung zu gewährleisten. Gesichert werden sowohl eingeschaltete, ausgeschaltete Cloud Server als auch Templates.

Mandantentrennung

Es erfolgt eine Trennung der Daten dergestalt, dass eine „Vermischung" mit Daten anderer Kunden der ACP und auch unbefugte Zugriffe Dritter (auch versehentlich) nicht möglich sind, u.a. durch

- Alle im Rechenzentrum verwendeten Netze werden in den Netzwerkkomponenten logisch voneinander getrennt.
- Physisch oder virtuell (VM) getrennte Systemumgebungen
- getrennte Datenbanken
- getrennte Ordnerstrukturen (Auftragsverarbeitung)
- separate Ordnerstruktur mit Berechtigungen

Verfügbarkeit und Belastbarkeit

ACP unterhält Notfallpläne für die Systeme und Einrichtungen, in denen Kundendaten verarbeitet werden. Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit umfassen insbesondere:

Schutz der Datensicherheitsräume

- Feuer nach DIN 4102-2 / F90, mit bauaufsichtlicher Zulassung
- Temperaturgrenzwerte und Luftfeuchte für 30 Minuten gem. EN 1047-2
- Rauchschutz nach DIN 18095
- unbefugter Zutritt / Einbruchhemmung WK II nach EN 1627
- Löschwassereintritt mit Wasserdichtigkeitsnachweis gem. EN 60529 / IP 56
- Staubdichtigkeit gemäß EN 60529
- Sabotage / Vandalismus
- EMV-Schutz
- Schutz gegen erhöhte Trümmerlasten

Brandschutzkonzept in Abstimmung mit der Branddirektion München

- Flucht und Rettungswege
- Raumbildender Brandschutz F90+
- Flächendeckende Brandmeldeanlagen gemäß VDE 0800 Teil 1, VDE 0833 Teil 1 u. 2,
- VDE 0100 Allg. Bestimmungen, DIN 14675 Brandmeldeanlagen-Aufbau,
- DIN 14661 Feuerwehrbedienfeld, VdS 2095 Richtlinien für Brandmeldeanlagen
- Feuerwehraufschaltung
- Aktive analoge Rauchansaugsysteme, mit dauerhafter Luftstromüberwachung
- (Brandfrüherkennungssystem)
- Automatische Gaslöschanlage

Kontinuierliche Überwachung von Kapazitäten

Die Kapazitäten werden kontinuierlich durch das Monitoring (Nagios, Veeam Monitor und vCenter) überwacht und lösen bei Unterschreitung bzw. Überschreitung der jeweilig festgelegten Schwellwerte Warnungen bzw. Alarme aus.

Diese Warnungen und Alarme werden mindestens einmal täglich beim täglichen Check ausgelesen und dann gegebenenfalls notwendige Maßnahmen eingeleitet.

Schutzmaßnamen für Angriffe von Dritten

Firewall - Übergänge von getrennten Netzen werden im Rechenzentrum durch Firewall-Systeme abgesichert. Es werden sowohl physische als auch virtuelle Firewall-Systeme verwendet. Bei allen eingesetzten Firewall-Systemen sind standardmäßig alle Übertragungswege deaktiviert. Es werden nur explizit benötigte IP-Adressenbereiche und Ports freigeschaltet, die vom Kunden über Ticket beantragt werden.

WAF - Zum Schutz von Web-Anwendungen wird eine Web Application Firewall (WAF) eingesetzt, die vor Angriffen über das Hypertext Transfer Protocol (HTTP) schützt.

DMZ - Einzelne in öffentlichen Netzen verfügbare Services werden zudem über DMZs zugänglich gemacht. Die in einer DMZ angeschlossenen Systeme werden dabei durch eine oder mehrere Firewalls gegen andere Netze abgeschirmt. Durch diese Trennung mittels DMZs werden zusätzliche Sicherheitszonen geschaffen.

Penetrationstests - Es werden regelmäßig Penetrationstests durchgeführt, bei denen ein umfassender Sicherheitstest von einzelnen öffentlich verfügbaren IP-Adressen auf Schwach-stellen überprüft werden.

Verschlüsselung - Applikationen die als Web-Seiten über öffentliche Netze genutzt werden, werden ausschließlich über verschlüsselte HTTPS Verbindungen zugänglich gemacht.

Anlage 5

„Datenschutzrelevante Punkte bei Nutzung der tisoware.APP“

Stand 01.09.2022

"App" bezeichnet das kodierte Symbol oder das Icon, einschließlich der darin enthaltenen Software, mit welcher ein Endnutzer auf Informationen und Funktionen aus der Softwarelösung von Atoria zugreifen kann. Die APP erscheint nach Download auf dem Smartphone, PC oder Tablet.

"Endnutzer" bezeichnet eine identifizierte oder identifizierbare natürliche Person, die z. B. als Mitarbeiter eines Unternehmens die App nutzt.

"Unternehmen" ist der Auftraggeber oder Arbeitgeber des Endnutzers und erwirbt durch Abschluss eines Lizenzvertrags mit Atoria die erforderlichen Lizenzen, um die Atoria.LÖSUNG für den internen Geschäftsbetrieb und für den Zugriff über die App durch

die Endnutzer zu nutzen bzw. nutzen zu lassen.

Kategorie der personenbezogenen Daten

Mit der App erhalten Sie als Endnutzer Informationen zu den in der Softwarelösung von Atoria abgelegten und verarbeiteten personenbezogenen Daten in Ihrem Unternehmen. Über die App können die Endnutzer diese personenbezogenen Daten ergänzen und darauf zugreifen.

Über die APP verarbeitete personenbezogene Daten sind damit nur solche Informationen, die in der vom Unternehmen lizenzierten Softwarelösung von Atoria.

entweder vom Unternehmen oder vom Endnutzer hinterlegt werden.

In Bezug auf diese personenbezogenen Daten handelt allein das Unternehmen als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO. Atoria verarbeitet diese Daten nur im Auftrag gemäß der mit dem Unternehmen geschlossenen vertraglichen Vereinbarung.

Abhängig von der vertraglichen Vereinbarung mit dem Unternehmen lassen sich über die App u. a. nachfolgend genannte weitere personenbezogene Daten abrufen und bearbeiten:

- Mitarbeiterstammdaten (z. B. Logindaten, Kennwort) und zeitwirtschaftliche Informationen
- Informationen aus der Personaleinsatzplanung = Dienstplan
- Informationen aus Antragswesen = Workflow
- Informationen zur Zeitbewertung = Buchungsprotokoll und Stempelkarte
- Systembezogene Informationen etc.

Stempelkarte, Dienstplan, Abwesenheitsworkflows, Workflow-Übersicht und Buchungsprotokoll und diverse vom Kunden definierte Buchungsfunktionalitäten wie Kommen-Gehen, Abfrage Zeitmodellwechsel, Projektwechsel. (Datenbankfelder: Online, Datum, Zeit, Meldecode, Funktion, Kostenstelle, Lohnart, Bereitschaftsdienst, Zeitmodell, Menücode, Projekt, Aktivität, Leistungsart)

Logging

In der App wird im Standard nichts protokolliert.

Routing-Hub

Die Kommunikation zwischen APP und Atoria-Backend wird über einen zentralen Cloud-Routing-Hub vermittelt. Im Routing-Hub wird hierbei die Kommunikation bzw. Vermittlung zum Kommunikationsmonitoring geloggt. Hierbei werden aber keine personenbezogenen Daten gespeichert, sondern lediglich die im Http-Header verfügbaren Informationen wie Routing-ID und die Device-ID. Diese Datensätze werden automatisiert nach vier Wochen gelöscht.

Die eigentlichen Inhalte (Http-Body) kann der Cloud-Routing-Hub nicht auslesen, da diese zwischen App und Atoria-Backend verschlüsselt sind.

Berechtigungen der App und Zwecke

Nur Berechtigungen, die für die Funktion der App zwingend erforderlich sind, werden eingefordert. Wird eine der Berechtigungen vom Endnutzer abgelehnt, stehen ggf. nicht alle Funktionen der App in vollem Umfang zur Verfügung.

Betriebssysteme

Die App unterstützt die Betriebssysteme iOS, Android und Windows (x64) und benötigt die folgenden Berechtigungen:

Kamera

Zum Einscannen des QR-Codes

Steuerungsmöglichkeiten des Zugriffs durch Endnutzer

Der Endnutzer kann beim ersten Start der Funktion „Kamera“ nach Installation der App zustimmen oder ablehnen, ob die App auf die Kamera seines mobilen Endgerätes zugreifen darf.

Bildergalerie

Um ggf. im Rahmen der manuellen Feedback-Funktion auf einen Screenshot zuzugreifen.

Steuerungsmöglichkeiten des Zugriffs durch Endnutzer

Der Endnutzer kann beim ersten Start der Funktion „Bildergalerie“ nach Installation der App zustimmen oder ablehnen, ob die App auf die Bildergalerie des mobilen Endgerätes zugreifen darf.

Push-Nachrichten

Im Kontext der App können lokale Push-Nachrichten generiert werden, z.B. technische Nachrichten wie Verarbeitung von Workflows und Offline-Buchungen oder auf den User bezogene Benachrichtigungen.

Zugriff auf personenbezogene Daten möglich?

Ja

Steuerungsmöglichkeiten des Zugriffs durch Endnutzer

Empfang kann abhängig vom Betriebssystem des mobilen Endgeräts gesteuert werden:

Bei iOS: Abfrage beim Endnutzer, ob er das Senden von Push-Benachrichtigungen erlaubt.

Bei Android: Erlaubnis zum Senden von Push-Benachrichtigungen ist standardmäßig eingeschaltet, kann aber per Einstellung ausgeschaltet werden

Datenspeicherung auf dem mobilen Endgerät

Auf dem mobilen Endgerät werden folgende personenbezogene Daten verschlüsselt (zum Teil nur für Offline-Buchungen = gepufferte Buchungen):

Firma, Personalnummer, Ausweis und PIN, Buchungs-Funktionen, Datum und Zeit der Buchung, Kostenstelle, Lohnart

Standortzugriff

Ja, möglich

Steuerungsmöglichkeiten des Zugriffs durch Administrator bzw. Endnutzer

Sofern seitens des Unternehmens in der Atoria.LÖSUNG gewünscht und aktiviert ist wird versucht die Position bei Buchungen zu ermitteln. Dies kann durch den Endnutzer am Endgerät über die Systemeinstellungen übersteuert werden.

Gibt es in der App, die Möglichkeit zur Kontaktaufnahme mit einem Support?

Der Endnutzer kann den Atoria.Support nach Aktivierung des App-Loggings via separatem Aufruf und Eingabe einer mitgeteilten Support-ID die Login-Daten der App übermitteln.

Werden Daten auf einer SD-Karte gespeichert?

Nein

Löschung der Daten

Personenbezogene Daten bei Offline-Buchungen (siehe vorherigen Abschnitt) werden automatisch nach erneuter Verbindung mit dem Server und erfolgreicher Übertragung vom mobilen Endgerät gelöscht. Als Endnutzer können Sie die App jederzeit eigenständig von Ihrem Endgerät löschen. Eventuell vorhandene Offline-Buchungen (Pufferungen) werden dadurch auch gelöscht. Bitte beachten Sie, dass die APP Sie als mitarbeitende Person bei Ihrem Unternehmen nur befähigt, auf einem bei Ihrem Unternehmen bereits eingerichteten Account zuzugreifen, um Ihre Daten ortsunabhängig bearbeiten und ergänzen zu können.

Die vollständige Löschung Ihres bereits eingerichteten User-Accounts ist daher nur in der Atoria.LÖSUNG des tisoware.PRODUKTES in Abstimmung mit Ihrem Unternehmen als Arbeitgeber möglich, da ihr Arbeitgeber die alleinige Verantwortung für das User-Management hat.