# Vereinbarung zur Auftragsverarbeitung

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

**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 tisoware Gesellschaft für Zeitwirtschaft mbH (nachfolgend „tisoware" oder „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 tisoware mit der Bereitstellung von Produkten und Services aus dem Produkt- und Serviceportfolio des Auftragnehmers im Bereich der Zeitwirtschaft (Zeiterfassung, Zutrittssicherung, Personaleinsatzplanung, Betriebsdatenerfassung, Maschinendatenerfassung, Videoanalyse, Reisekostenmanagement, Kantinendatenmanagement u. a.) beauftragt.

Bei der Erbringung der Leistungen durch tisoware oder durch sie beauftragte Unterauftragnehmer (Subunternehmer), wie z.B. Wartung der von tisoware installierten Software beim Auftraggeber vor Ort oder per Fernwartung oder bei dem Betrieb als Cloud-Lösung, kann ein in Berührung kommen mit personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden. Soweit dies der Fall ist, verarbeitet der Auftragnehmer personenbezogene Daten nur im Auftrag und nach Weisung des Auftraggebers.

Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 EU Datenschutz-Grundverordnung (DSGVO) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung. In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen.

## § 1 Gegenstand und Dauer der Vereinbarung

Der Auftragnehmer installiert, implementiert und wartet Softwaresysteme aus der Produktpalette der tisoware 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.

Die vertraglich vereinbarte Dienstleistung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit ausdrücklicher Zustimmung des Auftraggebers und unter den in Kapitel V der DSGVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieser Vereinbarung erfolgen.

Typische Wartungs- und Installationstätigkeiten umfassen:

- Installieren von Software
- Einspielen von Updates
- Schulung/Unterstützung der User
- Bearbeitung von Hotline Anfragen und Analyse von Anwendungen
- Reorganisation der Datenbank
- vom Auftraggeber speziell angeforderte Unterstützung

Der Auftraggeber ist im Rahmen dieser Vereinbarung 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 DSGVO und sonstiger Datenschutzvorschriften einzuhalten.

Der Auftrag ist im Rahmen des Projekts und ggf. daran anschließender Wartungs- und Supporttätigkeiten unbefristet erteilt und kann von beiden Parteien unter Berücksichtigung der gesetzlichen Fristen gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

## § 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

### Art und Zweck der Verarbeitung

Die Verarbeitung umfasst nach Art. 4 Nr. 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie die Analyse, das Ordnen, die Anpassung oder Veränderung, das Auslesen, das Abfragen, den Abgleich oder die Verknüpfung, das Löschen oder die Vernichtung.
Die Verarbeitung dient dem Zweck der Beratung, der Software-Installation und –Wartung sowie Supporttätigkeit des Auftragnehmers beim sowie für den Auftraggeber.

**Zusatz: Zweck der Verarbeitung bei Modul tisoware.eAU.**
Automatische, mitarbeiterbezogene Abfrage der elektronischen Arbeitsunfähigkeitsbescheinigung beim Server der GKV über Beginn und Dauer einer Arbeitsunfähigkeitsbescheinigung über eine von der ITSG zertifizierten Schnittstelle.

### Art der Daten

Dabei können die folgenden personenbezogenen Daten gem. Art. 4 Nr. 1 DSGVO verarbeitet werden:

- 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)
- 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, Geburtdatum,-Name,-Ort)
- Reisedaten in Verbindung mit Personendaten
- Kommunikationsdaten (z.B. Telefon/Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- und Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten

**Kategorien der betroffenen Personen**

Von der Verarbeitung betroffene natürliche Personen sind Beschäftigte i. S. d. § 26 Abs. 8 BDSG (neu).

## § 3 Rechte und Pflichten sowie Befugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen,

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich. Dies gilt auch für den Verzicht auf dieses Schriftformerfordernis. Ein Verzicht ist nicht möglich soweit das Gesetz die Schriftform zwingend vorschreibt.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmässigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherungsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

## § 4 Ansprechpartner des Auftraggebers sowie des Auftragnehmers

Weisungsempfangsberechtigte Ansprechpartner beim Auftragnehmer sind: Geschäftsleitung und IT-Abteilung tisoware, zu erreichen unter 0049 7121 9 66 50, datenschutz@tisoware.com.

Der Auftraggeber teilt dem Auftragnehmer die weisungsberechtigten Ansprechpartner des Auftraggebers und ggfs. Nachfolger bzw. Vertreter zeitnah und schriftlich oder elektronisch mit.

## § 5 Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. A DSGVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen und der Datenschutz-Folgenabschätzung (einschließlich einer etwaigen erforderlichen vorherigen Konsultation).

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die gem. § 4 benannten Ansprechpartner des Auftraggebers weiterzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28

Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort. (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung dieser Vereinbarung fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragter für den Datenschutz der Datenschutzbeauftragte der proALPHA Unternehmensgruppe bestellt. Er ist zu erreichen unter dataprotection@tisoware.com .

## § 6 Mitteilungspflichten des Auftragnehmers bei Störung der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im

Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und Art. 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. § 4 dieser Vereinbarung durchführen.

## § 7 Unterauftragsverhältnisse mit Subunternehmen

Die Beauftragung von Subunternehmen zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmen in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen den Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).
Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zur Zeit sind für den Auftragnehmer die als Anlage mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt (Anlage 2). Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 Satz 2 DSGVO).

Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

## § 8 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Die festzulegenden technischen und organisatorischen Maßnahmen sind der Anlage zu entnehmen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftragnehmer unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich / elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieser Vereinbarung aufzubewahren.

## § 9 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags bzw. der Geschäftsbeziehung

Nach Abschluss der vertraglichen Arbeiten bzw. Leistungen oder dem Ende der Geschäftsbeziehung hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten,

Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben.

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

## § 10 Vergütung

Im Rahmen des gültigen Software-Wartungsvertrags erhalten Sie die DSGVO-konforme Update-Version ohne Berechnung. Die Inanspruchnahme von Installations-, Implementierungs- oder Schulungsdienstleistungen berechnen wir gemäß vereinbarter Konditionen.

Für die Ermöglichung von datenschutzbezogenen Mitwirkungspflichten wie Kontrollen durch den Auftraggeber kann der Auftragnehmer einen vorher festzulegenden Vergütungsanspruch geltend machen.

## § 11 Haftung

Auf Art. 82 DSGVO wird verwiesen.

## § 12 Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

# Anlage 1
# Subunternehmer - Zusammenstellung von Subunternehmern, die im Unterauftragsverhältnis tätig werden können:

1. **dormakaba** Deutschland GmbH, Access Solutions DACH
   DORMA Platz 1, 58256 Ennepetal, Deutschland
2. **PCS** Systemtechnik GmbH
   Pfälzer-Wald-Str. 36, 81539 München
3. **DATAFOX GMBH**
   Dermbacher Straße 12-14, 36419 Geisa
4. **FORSIS GmbH**
   Schwanenstraße 5, 88214 Ravensburg
5. **IDENTA Ausweissysteme GmbH**
   Steinkirchring 16, 78056 Villingen-Schwenningen
6. **ACP IT Solutions AG**
   Carl-Jordan-Str. 18a, 83059 Kolbermorr
7. **payroll GmbH**
   Colonia-Allee 13 – 15, 51067, Köln
8. **profibu GmbH**
   Colonia-Allee 13 – 15, 51067, Köln

## Art der Tätigkeiten(en):

1. – 4.: Lieferung von Hardware aus der Produktpalette des Lieferanten, Eventuelle Installations- und Entstörungsmaßnahmen

5. : Herstellung von Ausweismedien

6. Bereitstellung cloud-basierter Dienst: Infrastructure as a Service bei Cloud Kunden

7. Automatische, mitarbeiterbezogene Abfrage der elektronischen Arbeitsunfähigkeitsbescheinigung beim Server der GKV über Beginn und Dauer einer Arbeitsunfähigkeitsbescheinigung über eine von der ITSG zertifizierten Schnittstelle

8. Bereitstellung cloud-basierter Dienst: Web-Server (für Dakota Software) bei tisoware.eAU Kunden

# Anlage 2
# „technische und organisatorische Maßnahmen nach Art. 32 DSGVO“ (TOM), Stand 01.06.2019

## 1. Vertraulichkeit

### Zutrittskontrolle

Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden:

- 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 tisoware 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 tisoware eigenen Rechner durch. Der tisoware Rechner ist Passwort geschützt und verschlüsselt.

**Zugangskontrolle**

Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -verfahren gehindert werden:

- 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
- Keine schriftliche Hinterlegung der Passwörter (Ausnahme: verschlossene Umschläge im Tresor)

**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:

- Berechtigungskonzept
- Sicherung von Datenträgern nach Erstellung im Tresor
- Differenzierte Zugriffsberechtigungen auf Dateien, Datensätze, Datenfelder und Anwendungsprogramme
- Protokollierung der Zugriffe (Datenbanken, File- und Kundensysteme)
- tisoware Notebooks sind passwortgeschützt
- Bereiche mit personenbezogenen Daten sind auf externen Medien durch bestimmte Software verschlüsselt

**Trennungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Einhaltung von Aufbewahrungsfristen und anschließende Löschung der zur Verfügung gestellten Daten
- Funktionstrennung: Trennung zwischen Test- und Produktivsystemen
- Getrennte IT-Netze für unterschiedliche Verarbeitungszwecke

**Pseudonymisierung**

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person

zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

## 2. Integrität

### 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:

- Einsatz einer Firewall (Hardware/Software)
- Durchgängige Nutzung eines Virtual Private Network (VPN)
- Content Filter
- Viren-Schutz (Server und Clients)
- SPAM-Schutz
- Datenschutzgerechte Papierentsorgung durch Reißwolf und über eine spezialisierte Entsorgungsfirma
- Datenschutzgerechte Datenträgerentsorgung über eine spezialisierte Entsorgungsfirma

### Eingabekontrolle

Maßnahmen, die es überprüfbar und feststellbar machen, von wem Daten eingegeben, verändert und entfernt wurden:

- Protokollierung von Datenerfassung, -veränderung und -entfernung
- Datenpflege nur durch tisoware Mitarbeiter

## 3. Verfügbarkeit und Belastbarkeit

### Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- 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
- Unterbrechungsfreie Stromversorgung (USV) in den Serverräumen im Einsatz
- Überspannungsschutzeinrichtungen in den Serverräumen im Einsatz
- Klimaanlage in den Serverräumen installiert
- Regelmäßige Datensicherung

- Redundante Serverräume
- Durchgängiger Einsatz von Virenscanner und Firewall mit ständigen Updates (bei Servern und Clients)

**Rasche Wiederherstellbarkeit**
Die rasche Wiederherstellbarkeit ist aufgrund unserer Infrastruktur (Sandboxing mit VM-Ware) und der Art und Weise unserer Datensicherung gegeben. Innerhalb eines Tages sind die kritischen Systeme wieder aus unseren Backups herstellbar. Außerdem können kritische Systeme jederzeit auf andere Maschinen umziehen, somit auch gegen Hardwareausfälle gesichert.

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Das Datenschutz-Management definiert und baut kontinuierlich im laufenden Betrieb die Definition von Verantwortlichkeiten, Strukturen und Prozesse auf und aus. Dies wird in einer Verfahrensbeschreibung strukturiert dokumentiert, damit wir die regelmäßige

Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sicherstellen können.

- Vorhandene Verfahren, mit Hilfe dessen regelmäßig die Wirksamkeit der technischen und organisatorischen Maßnahmen überprüft, evaluiert und bewertet wird, wie internes jährliches Audit sowie jährliche ISO 27001-Prüfung bzw. Rezertifizierung.
- Regelmäßige Prüfung durch unseren Datenschutzbeauftragen findet jährlich statt
- IT Health Checks und Penetrationstests
- Durchführung von Notfallübungen

**Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DSGVO)

***„Privacy by Design" und „Privacy by Default"*** *- Ein umfangreiches Rechte Management ist in den tisoware-Anwendungen ebenso wie in CRM- und DMS-Anwendungen, die wir nutzen, vorhanden; mit den tisoware-Applikationen sind ab Version 10.6 in Verbindung mit ADS die Vorkehrungen getroffen.*

**Auftragskontrolle**

Maßnahmen, die sichern, dass Daten nur entsprechend den Anweisungen des Auftraggebers verarbeitet werden:

- Durchführung von Aufträgen anhand von schriftlichen Aufträgen
- Dokumentation aller Aufträge
- Eindeutige Vertragsgestaltung

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

ACP IT Solutions AG (im weiteren ACP genannt) stellt Leistungen für tisoware 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 Schwachstellen überprüft werden.

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

## Anlage 3
## „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 tisoware zugreifen kann. Die tisoware.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 tisoware die erforderlichen Lizenzen, um die tisoware.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 tisoware abgelegten und verarbeiteten personenbezogenen Daten in Ihrem Unternehmen. Über die App können die Endnutzer diese personenbezogenen Daten ergänzen und darauf zugreifen.

Über die tisoware.APP verarbeitete personenbezogene Daten sind damit nur solche Informationen, die in der vom Unternehmen lizenzierten Softwarelösung von tisoware 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. tisoware 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 tisoware.APP und tisoware-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 tisoware-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 tisoware.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 tisoware.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 tisoware.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 tisoware.LÖSUNG in Abstimmung mit Ihrem Unternehmen als Arbeitgeber möglich, da ihr Arbeitgeber die alleinige Verantwortung für das User-Management hat.