

Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO über die Verarbeitung von Arbeitszeitdaten mit dem Dienst „Zeitnachweis“

Fassung 2026-10-14 · Verbindlich ist allein die deutsche Fassung.

Hinweis zum Vertragsschluss

Dieser Auftragsverarbeitungsvertrag ist ein standardisierter Vertragstext (Muster). Er wird zwischen dem Arbeitgeber und der Desatec Systems GmbH auf elektronischem Weg geschlossen, indem die für den Arbeitgeber handelnde Person bei der Registrierung des Arbeitgeber-Kontos das Kontrollkästchen „Ich habe den Auftragsverarbeitungsvertrag gelesen und stimme ihm zu“ aktiviert (Art. 28 Abs. 9 DSGVO: elektronisches Format).

Zeitpunkt der Annahme und Fassungsnummer werden dauerhaft beim Arbeitgeber-Konto gespeichert. Die zum Zeitpunkt der Annahme gültige Fassung ist für das jeweilige Vertragsverhältnis maßgeblich; frühere Fassungen werden von Desatec Systems archiviert und dem Arbeitgeber auf Anfrage als PDF bereitgestellt. Ein händisch unterzeichnetes Exemplar ist nicht erforderlich, kann auf Wunsch des Arbeitgebers aber zusätzlich ausgetauscht werden.

Vertragsparteien

Verantwortlicher („Auftraggeber“)
Der Arbeitgeber, der ein Arbeitgeber-Konto im Dienst „Zeitnachweis“ registriert hat, mit der bei der Registrierung angegebenen Firma und E-Mail-Adresse sowie den im Konto hinterlegten Firmendaten, vertreten durch die Person, die das Konto angelegt und diesen Vertrag angenommen hat.

Auftragsverarbeiter („Auftragnehmer“)
Desatec Systems GmbH
Adolf-Hoyer-Straße 5, 37079 Göttingen, Deutschland
vertreten durch den Geschäftsführer André Runzer
Registergericht: Amtsgericht Göttingen, HRB 201074
Datenschutzbeauftragter: Alexander Lemke, datenschutz@desatec.systems

Präambel

Der Auftraggeber nutzt den Dienst „Zeitnachweis“ (Mobile App für Beschäftigte und Arbeitgeber-Bereich im Web, nachfolgend „Dienst“), um Arbeitszeiten seiner Beschäftigten aufzuzeichnen, zu prüfen, zu korrigieren und daraus Arbeitszeitznachweise zu erstellen. Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien nach Art. 28 DSGVO und ergänzt das zwischen den Parteien bestehende Nutzungsverhältnis über den Dienst (nachfolgend „Hauptvertrag“). Bei Widersprüchen zu Fragen des Datenschutzes geht dieser Vertrag dem Hauptvertrag vor.

Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO für die Arbeitszeitdaten seiner Beschäftigten. Der Auftragnehmer ist Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO. Für die Daten des Arbeitgeber-Kontos selbst (Firmen- und Zugangsdaten, Vertragsabwicklung) ist der Auftragnehmer eigenständig Verantwortlicher; hierzu gilt die Datenschutzerklärung des Dienstes.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Bereitstellung und der Betrieb des Dienstes „Zeitnachweis“ durch den Auftragnehmer für den Auftraggeber, insbesondere die Entgegennahme, Speicherung, Versionierung, Auswertung und Ausgabe von Arbeitszeitdaten, die Beschäftigte des Auftraggebers mit der App erfassen oder die der Auftraggeber im Arbeitgeber-Bereich eingibt oder korrigiert. Umfang, Art und Zweck der Verarbeitung ergeben sich aus Anlage 1 und aus der Leistungsbeschreibung des Hauptvertrags.

(2) Der Auftragnehmer verarbeitet die Daten ausschließlich im Auftrag und nach Weisung des

Auftraggebers im Sinne von Art. 28 DSGVO. Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt; insbesondere werden Arbeitszeitdaten nicht zu Werbe-, Analyse- oder Profilbildungszwecken ausgewertet und nicht an Dritte verkauft oder weitergegeben.

(3) Die Dauer dieses Vertrags entspricht der Dauer des Hauptvertrags. Er beginnt mit der Annahme bei der Registrierung des Arbeitgeber-Kontos und endet mit der Beendigung des Hauptvertrags, insbesondere mit der Löschung des Arbeitgeber-Kontos. § 10 (Löschung und Rückgabe) und § 13 (Schlussbestimmungen) gelten über das Vertragsende hinaus.

(4) Die Verarbeitung findet ausschließlich in der Bundesrepublik Deutschland statt. Eine Verarbeitung in einem anderen Mitgliedstaat der Europäischen Union oder des Europäischen Wirtschaftsraums bedarf der vorherigen Information des Auftraggebers in Textform; eine Übermittlung in ein Drittland oder an eine internationale Organisation findet nicht statt und bedarf, sollte sie künftig erforderlich werden, der vorherigen Zustimmung des Auftraggebers sowie der Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, Kreis der Betroffenen

(1) Zweck der Verarbeitung ist die Erfüllung der gesetzlichen Pflicht des Auftraggebers zur Aufzeichnung der Arbeitszeit seiner Beschäftigten (insbesondere § 16 Abs. 2 ArbZG, § 17 MiLoG, § 3 ArbSchG in der Auslegung durch BAG, Beschluss vom 13.09.2022 – 1 ABR 22/21), die Prüfung der Aufzeichnungen auf Einhaltung arbeitszeitrechtlicher Vorgaben, die Erstellung monatlicher Arbeitszeitznachweise (PDF) und von Exporten für die Entgeltabrechnung (CSV) sowie die Sicherstellung der Nachvollziehbarkeit nachträglicher Änderungen.

(2) Die Art der Verarbeitung umfasst das Erheben über die App-Schnittstelle, das Speichern, das Ordnen, das Verändern durch Anlegen neuer Versionen, das Auslesen, das Abfragen, das Verwenden zur Berechnung von Summen und Prüfhinweisen, das Bereitstellen an den Auftraggeber und an die jeweils betroffene Person, das Einschränken sowie das Löschen.

(3) Art der Daten und Kreis der betroffenen Personen sind in Anlage 1 abschließend festgelegt. Der Auftraggeber stellt sicher, dass über den Dienst keine anderen als die dort genannten Datenarten verarbeitet werden; insbesondere eignet sich der Dienst nicht für Gesundheitsdaten oder sonstige besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO. Freitextfelder (Begründungen, Bemerkungen) sind vom Auftraggeber und seinen Beschäftigten entsprechend sparsam zu nutzen.

(4) Der Dienst erhebt keine Standortdaten, keine Bildschirm- oder Kamerainhalte, keine Kontakt- oder Nutzungsstatistiken und nimmt keine Verhaltens- oder Leistungsbewertung vor. Der Auftragnehmer wird solche Funktionen nicht ohne ausdrückliche Vertragsänderung einführen.

§ 3 Verantwortlichkeit und Weisungsrecht des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, insbesondere für das Vorliegen einer Rechtsgrundlage gegenüber seinen Beschäftigten (§ 26 BDSG, Art. 6 Abs. 1 lit. c DSGVO), für die Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO gegenüber den Beschäftigten, für die Beteiligung einer etwaigen Arbeitnehmervertretung sowie für die Wahrung der Rechte der betroffenen Personen allein verantwortlich. Der Auftragnehmer erbringt keine Rechtsberatung.

(2) Der Auftraggeber erteilt alle Weisungen grundsätzlich durch die Nutzung der im Dienst bereitgestellten Funktionen (z. B. Anlegen und Deaktivieren von Beschäftigten, Erzeugen und Löschen von Registrierungs-codes, Korrigieren und Löschen von Zeiteinträgen mit Begründung, Export, Löschung des Kontos). Dieser Vertrag sowie die Leistungsbeschreibung des Hauptvertrags enthalten die allgemeinen Weisungen.

(3) Darüber hinausgehende Einzelweisungen erteilt der Auftraggeber in Textform (z. B. E-Mail an datenschutz@desatec.systems). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Weisungsberechtigt sind die Inhaber des Arbeitgeber-Kontos sowie die vom Auftraggeber im Dienst angelegten weiteren Zugänge im Rahmen ihrer Rolle; Änderungen der weisungsberechtigten Personen

nimmt der Auftraggeber selbst im Dienst vor.

(4) Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Der Auftragnehmer kann für ihre Umsetzung eine angemessene Vergütung verlangen, soweit sie nicht zur Abstellung eines Verstoßes in seinem Verantwortungsbereich erforderlich sind.

(5) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Er ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis der Auftraggeber sie bestätigt oder ändert.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 4 Pflichten des Auftragnehmers

(1) Weisungsgebundenheit. Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt er dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Vertraulichkeit. Der Auftragnehmer setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet wurden (Art. 28 Abs. 3 Satz 2 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO) und vor Aufnahme ihrer Tätigkeit mit den für sie relevanten Datenschutzbestimmungen vertraut gemacht worden sind. Die Verpflichtung besteht nach Beendigung der Tätigkeit fort. Der Zugriff auf Produktivdaten ist auf die für Betrieb und Fehlerbehebung zwingend erforderlichen Personen beschränkt.

(3) Datenschutzbeauftragter. Der Auftragnehmer hat einen Datenschutzbeauftragten benannt: Alexander Lemke, Adolf-Hoyer-Straße 5, 37079 Göttingen, datenschutz@desatec.systems. Wechsel werden dem Auftraggeber auf der Datenschutzseite des Dienstes bekannt gegeben.

(4) Sicherheit der Verarbeitung. Der Auftragnehmer trifft alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen; Einzelheiten regelt § 5 und Anlage 2.

(5) Trennung. Daten verschiedener Auftraggeber werden logisch getrennt (mandantenbezogene Zuordnung jedes Datensatzes); ein Zugriff über die Grenzen eines Arbeitgeber-Kontos hinweg ist technisch ausgeschlossen.

(6) Integrität und Nachvollziehbarkeit. Zeiteinträge werden serverseitig ausschließlich anfügend („append-only“) gespeichert: Jede Änderung oder Löschung erzeugt eine neue Version mit Urheber, Zeitpunkt und Begründung; keine Version wird überschrieben oder entfernt. Der Auftragnehmer nimmt an Zeiteinträgen keine inhaltlichen Änderungen vor; dies obliegt ausschließlich dem Auftraggeber und seinen Beschäftigten.

(7) Transparenz gegenüber Beschäftigten. Der Auftragnehmer stellt sicher, dass jede betroffene Person über die App die sie betreffenden, beim Auftragnehmer gespeicherten Zeiteinträge einschließlich der Korrekturen des Auftraggebers abrufen kann. Dies unterstützt den Auftraggeber bei der Erfüllung von Art. 15 DSGVO und ersetzt nicht dessen eigene Pflichten.

(8) Zusammenarbeit mit Aufsichtsbehörden. Der Auftragnehmer arbeitet auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen und informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie diesen Auftrag betreffen, es sei denn, eine Mitteilung ist ihm gesetzlich oder behördlich untersagt.

(9) Verfahrensverzeichnis. Der Auftragnehmer führt ein Verzeichnis aller Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dem Auftraggeber die ihn betreffenden Angaben auf Anfrage zur Verfügung.

(10) Gefährdung der Daten. Werden die Daten des Auftraggebers beim Auftragnehmer durch

Maßnahmen Dritter (etwa Pfändung, Beschlagnahme, Insolvenzverfahren) gefährdet, informiert der Auftragnehmer den Auftraggeber unverzüglich und weist alle Beteiligten darauf hin, dass die Verfügungsbefugnis über die Daten ausschließlich beim Auftraggeber liegt.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat vor Beginn der Verarbeitung die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen umgesetzt und dokumentiert. Sie gewährleisten unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen ein dem Risiko angemessenes Schutzniveau (Art. 32 DSGVO), insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf alternative Maßnahmen umsetzen, sofern das Sicherheitsniveau der Anlage 2 nicht unterschritten wird. Wesentliche Änderungen dokumentiert der Auftragnehmer; die jeweils aktuelle Fassung der Anlage 2 ist Bestandteil der unter der Adresse des Dienstes veröffentlichten Fassung dieses Vertrags. Eine Absenkung des Schutzniveaus bedarf der Zustimmung des Auftraggebers.

(3) Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen regelmäßig, mindestens jährlich sowie anlassbezogen nach sicherheitsrelevanten Änderungen, und dokumentiert das Ergebnis.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung (Art. 28 Abs. 2 Satz 1 DSGVO), die in Anlage 3 aufgeführten Unterauftragsverarbeiter für die dort genannten Leistungen einzusetzen.

(2) Unterauftragsverhältnisse im Sinne dieses Vertrags sind solche Leistungen, die sich unmittelbar auf die Verarbeitung der Auftragsdaten beziehen. Nicht dazu gehören Nebenleistungen wie Telekommunikations-, Post- und Transportdienste, Wartung ohne Zugriffsmöglichkeit auf Auftragsdaten, Reinigungs- oder Bewachungsdienste sowie die Beschaffung von Hard- und Software. Der Auftragnehmer stellt auch insoweit durch vertragliche Vereinbarungen und Kontrollen sicher, dass Vertraulichkeit und Sicherheit der Daten gewahrt bleiben.

(3) Beabsichtigt der Auftragnehmer die Hinzuziehung eines weiteren oder die Ersetzung eines bestehenden Unterauftragsverarbeiters, informiert er den Auftraggeber mindestens 30 Tage vor dem Einsatz in Textform (E-Mail an die Konto-Adresse) und veröffentlicht die geänderte Anlage 3. Der Auftraggeber kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt.

(4) Im Fall eines begründeten Widerspruchs bemühen sich die Parteien um eine einvernehmliche Lösung. Gelingt dies nicht innerhalb von 14 Tagen, ist jede Partei berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 14 Tagen in Textform außerordentlich zu kündigen; § 10 gilt entsprechend. Bei außergewöhnlichen Umständen, die ein Zuwarten unzumutbar machen (z. B. Ausfall eines Unterauftragsverarbeiters aus Sicherheitsgründen), verkürzt sich die Frist nach Absatz 3 auf eine angemessene Frist; der Auftragnehmer begründet dies.

(5) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter durch Vertrag nach Art. 28 Abs. 4 DSGVO auf dieselben Datenschutzpflichten, die in diesem Vertrag festgelegt sind, insbesondere auf hinreichende Garantien für technische und organisatorische Maßnahmen. Er prüft vor dem Einsatz und danach regelmäßig deren Einhaltung. Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

(6) Unterauftragsverarbeiter mit Sitz oder Verarbeitung außerhalb des Europäischen Wirtschaftsraums werden nicht eingesetzt. Sollte dies künftig beabsichtigt sein, gilt zusätzlich § 1 Abs. 4.

§ 7 Unterstützungspflichten des Auftragnehmers

(1) Rechte betroffener Personen. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) zu beantworten. Hierzu stellt der Dienst dem Auftraggeber insbesondere Funktionen zur Einsicht, zur begründeten Korrektur, zum Export in gängigen Formaten (PDF, CSV) und zur Deaktivierung von Beschäftigten bereit. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, verweist dieser sie unverzüglich an den Auftraggeber und leitet das Ersuchen innerhalb von drei Werktagen an den Auftraggeber weiter; er beantwortet Ersuchen nicht selbst, es sei denn, der Auftraggeber weist ihn dazu an.

(2) Art. 32 bis 36 DSGVO. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten zur Sicherheit der Verarbeitung (Art. 32), zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33) und an betroffene Personen (Art. 34), bei der Datenschutz-Folgenabschätzung (Art. 35) sowie bei der vorherigen Konsultation der Aufsichtsbehörde (Art. 36). Hierzu stellt er insbesondere die Beschreibung der Verarbeitung (Anlage 1), die technischen und organisatorischen Maßnahmen (Anlage 2) und die Unterauftragsverarbeiter (Anlage 3) zur Verfügung.

(3) Für Unterstützungsleistungen, die über die im Dienst bereitgestellten Funktionen und die gesetzlichen Pflichten des Auftragnehmers hinausgehen und nicht auf einem Fehlverhalten des Auftragnehmers beruhen, kann der Auftragnehmer eine angemessene Vergütung nach Aufwand verlangen; er kündigt dies vorher an.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO, die Auftragsdaten betrifft oder betreffen kann, unverzüglich nach Bekanntwerden, spätestens jedoch innerhalb von 48 Stunden, in Textform an die E-Mail-Adresse des Arbeitgeber-Kontos. Die Frist des Art. 33 Abs. 1 DSGVO für den Auftraggeber bleibt hiervon unberührt; der Auftragnehmer wird die Meldung so früh abgeben, dass der Auftraggeber sie einhalten kann, und Informationen bei Bedarf schrittweise nachreichen.

(2) Die Meldung enthält, soweit bereits bekannt, mindestens:

- eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze,
- Zeitpunkt oder Zeitraum des Vorfalls und Zeitpunkt der Feststellung,
- die wahrscheinlichen Folgen der Verletzung,
- die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und zur Abmilderung nachteiliger Auswirkungen,
- Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle.

(3) Der Auftragnehmer dokumentiert den Vorfall, sichert Beweise, ergreift unverzüglich die zur Eindämmung und Behebung erforderlichen Maßnahmen und stimmt sich mit dem Auftraggeber über weitere Schritte ab. Eine Information der Aufsichtsbehörde oder der betroffenen Personen nimmt der Auftragnehmer nur auf Weisung des Auftraggebers oder aufgrund eigener gesetzlicher Pflicht vor.

(4) Entsprechendes gilt für erhebliche Störungen des Betriebsablaufs, den Verdacht einer Datenschutzverletzung oder andere Unregelmäßigkeiten bei der Verarbeitung von Auftragsdaten.

§ 9 Nachweis- und Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO und aus diesem Vertrag zur Verfügung. Der Nachweis kann insbesondere erfolgen durch die Dokumentation der technischen und organisatorischen Maßnahmen

(Anlage 2), aktuelle Testate oder Prüfberichte unabhängiger Stellen (einschließlich der dem Auftragnehmer von seinen Unterauftragsverarbeitern bereitgestellten Prüfberichte, soweit deren Weitergabe zulässig ist), Selbstauskünfte in Textform sowie die Einhaltung genehmigter Verhaltensregeln oder Zertifizierungen nach Art. 40, 42 DSGVO.

(2) Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrags selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer zu überprüfen (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Vor-Ort-Prüfungen werden mit einer Ankündigungsfrist von mindestens 14 Tagen während der üblichen Geschäftszeiten durchgeführt, erfolgen ohne Störung des Betriebsablaufs, unter Wahrung der Betriebs- und Geschäftsgeheimnisse des Auftragnehmers und der Vertraulichkeit der Daten anderer Auftraggeber und sind auf eine Prüfung pro Kalenderjahr beschränkt. Anlassbezogene Prüfungen nach einer Datenschutzverletzung oder auf Verlangen einer Aufsichtsbehörde sind hiervon ausgenommen. Der Auftragnehmer kann einem Prüfer widersprechen, der in einem unmittelbaren Wettbewerbsverhältnis zu ihm steht.

(3) Prüfungen in den Rechenzentren der Unterauftragsverarbeiter erfolgen nach deren jeweiligen Regelungen; insoweit stellt der Auftragnehmer dem Auftraggeber die verfügbaren Prüfberichte und Zertifikate zur Verfügung.

(4) Der Aufwand des Auftragnehmers für Vor-Ort-Prüfungen wird vom Auftraggeber nach dem vorab mitgeteilten Stundensatz vergütet, es sei denn, die Prüfung ergibt einen erheblichen Verstoß des Auftragnehmers gegen diesen Vertrag oder sie ist anlassbezogen im Sinne von Absatz 2 Satz 3. Jede Partei trägt im Übrigen ihre eigenen Kosten.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Während der Vertragslaufzeit kann der Auftraggeber die Auftragsdaten jederzeit über die Exportfunktionen des Dienstes (monatliche Arbeitszeitznachweise als PDF, Abrechnungsexport als CSV, Gesamtexport des Kontos) in gängigen, maschinenlesbaren Formaten abrufen. Eine Löschung einzelner Zeiteinträge erfolgt innerhalb des Dienstes nach dem Prinzip der Versionierung (Löschvermerk mit Begründung); eine physische Entfernung einzelner Einträge während der Laufzeit ist aus Gründen der Nachweisbarkeit nicht vorgesehen.

(2) Nach Beendigung des Hauptvertrags löscht der Auftragnehmer sämtliche Auftragsdaten einschließlich Kopien, sofern nicht eine Verpflichtung zur Speicherung nach dem Recht der Union oder der Bundesrepublik Deutschland besteht. Die Beendigung durch Löschung des Arbeitgeber-Kontos im Dienst gilt als Weisung zur Löschung; der Dienst bietet dem Auftraggeber vor der Löschung einen vollständigen Export an und weist auf die Aufbewahrungspflichten hin. Die Löschung aus den Produktivsystemen erfolgt unmittelbar, die Löschung aus Datensicherungen spätestens mit Ablauf des Sicherungszyklus nach Anlage 2 (31 Tage); bis dahin werden Sicherungen nicht zur Wiederherstellung einzelner Konten verwendet.

(3) Die gesetzlichen Aufbewahrungspflichten für Arbeitszeitaufzeichnungen (insbesondere mindestens zwei Jahre nach § 16 Abs. 2 ArbZG und § 17 Abs. 2 MiLoG, bei Lohnunterlagen gegebenenfalls länger nach § 147 AO, § 257 HGB) treffen ausschließlich den Auftraggeber. Der Auftraggeber ist verpflichtet, die Daten vor Beendigung des Hauptvertrags zu exportieren und selbst aufzubewahren; der Auftragnehmer schuldet nach Vertragsende keine Aufbewahrung. Wünscht der Auftraggeber eine Aufbewahrung durch den Auftragnehmer über das Vertragsende hinaus, bedarf dies einer gesonderten Vereinbarung.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen (z. B. Protokolle, Angaben zur Annahme dieses Vertrags, Nachweise der Löschung), bewahrt der Auftragnehmer entsprechend den gesetzlichen Fristen über das Vertragsende hinaus auf. Auf Verlangen bestätigt der Auftragnehmer dem Auftraggeber die Löschung in Textform.

§ 11 Haftung

(1) Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Der Auftragnehmer haftet

danach nur für Schäden, die durch eine Verarbeitung verursacht wurden, bei der er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung oder entgegen rechtmäßig erteilter Weisungen des Auftraggebers gehandelt hat.

(2) Im Innenverhältnis haftet jede Partei für den Teil des Schadens, der auf ihren Verantwortungsbeitrag entfällt (Art. 82 Abs. 5 DSGVO). Eine im Hauptvertrag vereinbarte Haftungsregelung gilt auch für diesen Vertrag; die Haftung für Vorsatz, grobe Fahrlässigkeit, die Verletzung von Leben, Körper oder Gesundheit sowie nach zwingendem Recht bleibt unberührt.

(3) Der Auftraggeber stellt den Auftragnehmer von Ansprüchen Dritter frei, die darauf beruhen, dass der Auftraggeber die Verarbeitung ohne ausreichende Rechtsgrundlage veranlasst, seinen Informationspflichten nicht nachgekommen ist oder rechtswidrige Weisungen erteilt hat.

(4) Geldbußen nach Art. 83 DSGVO trägt jede Partei selbst, soweit sie gegen sie verhängt werden.

§ 12 Dauer, Kündigung, Änderungen

(1) Dieser Vertrag ist untrennbar an den Hauptvertrag gekoppelt und kann nicht isoliert gekündigt werden. Die Kündigung oder sonstige Beendigung des Hauptvertrags beendet zugleich diesen Vertrag; umgekehrt gilt eine wirksame außerordentliche Kündigung dieses Vertrags zugleich als Kündigung des Hauptvertrags.

(2) Jede Partei kann diesen Vertrag aus wichtigem Grund außerordentlich kündigen, insbesondere wenn die andere Partei schwerwiegend oder trotz Abmahnung wiederholt gegen Datenschutzvorschriften oder diesen Vertrag verstößt, der Auftragnehmer eine rechtmäßige Weisung dauerhaft nicht ausführt oder dem Auftraggeber Kontrollrechte vertragswidrig verweigert.

(3) Der Auftragnehmer kann diesen Vertrag anpassen, wenn dies aufgrund geänderter Rechtslage, Rechtsprechung, behördlicher Vorgaben oder Änderungen des Dienstes erforderlich ist. Änderungen werden dem Auftraggeber mindestens 30 Tage vor Inkrafttreten in Textform an die E-Mail-Adresse des Arbeitgeber-Kontos angekündigt und unter der Adresse des Dienstes veröffentlicht. Widerspricht der Auftraggeber nicht innerhalb von 30 Tagen nach Zugang der Ankündigung in Textform, gilt die geänderte Fassung als angenommen; hierauf weist der Auftragnehmer in der Ankündigung besonders hin. Widerspricht der Auftraggeber, gilt die bisherige Fassung fort; beide Parteien können den Hauptvertrag in diesem Fall mit einer Frist von 14 Tagen kündigen. Änderungen, die das Schutzniveau nur erhöhen oder Anlage 3 betreffen (§ 6), können ohne Widerspruchsverfahren erfolgen.

(4) Eine spätere Annahme einer neuen Fassung durch eine weisungsberechtigte Person des Auftraggebers im Dienst ersetzt die bisherige Fassung mit Wirkung für die Zukunft.

§ 13 Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist Göttingen, sofern der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder keinen allgemeinen Gerichtsstand in Deutschland hat. Zwingende gesetzliche Zuständigkeiten bleiben unberührt.

(2) Dieser Vertrag wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Die Annahme erfolgt durch Aktivieren des entsprechenden Kontrollkästchens bei der Registrierung des Arbeitgeber-Kontos; der Auftragnehmer protokolliert Zeitpunkt (UTC), Fassungsnummer und das annehmende Konto und stellt dem Auftraggeber diese Angaben im Arbeitgeber-Bereich sowie die angenommene Fassung als PDF zur Verfügung. Die annehmende Person sichert zu, zur Vertretung des Auftraggebers berechtigt zu sein. Änderungen und Ergänzungen dieses Vertrags einschließlich dieser Klausel bedürfen der Schriftform oder der Textform (z. B. E-Mail), wobei ausdrücklich kenntlich zu machen ist, dass es sich um eine Änderung dieses Vertrags handelt; § 12 Abs. 3 bleibt unberührt.

(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Anstelle der unwirksamen Bestimmung

gilt diejenige wirksame Regelung als vereinbart, die dem Zweck der unwirksamen Bestimmung und den Anforderungen des Art. 28 DSGVO am nächsten kommt.

(4) Dieser Vertrag ist in deutscher Sprache verfasst; allein die deutsche Fassung ist verbindlich. Übersetzungen oder Zusammenfassungen in anderen Sprachen dienen nur dem Verständnis.

(5) Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrags.

Anlagen

Anlage 1 – Gegenstand, Art und Zweck der Verarbeitung, Art der Daten, Kreis der Betroffenen

1. Gegenstand und Zweck

Betrieb des Dienstes „Zeitnachweis“ zur Aufzeichnung der Arbeitszeit der Beschäftigten des Auftraggebers, zur Prüfung der Aufzeichnungen auf arbeitszeitrechtliche Hinweise (Pausen, Höchstarbeitszeit, Ruhezeiten, vergessene Ausstempelungen, verspätete Aufzeichnung), zur Erstellung monatlicher Arbeitszeitznachweise (PDF) und von Exporten für die Entgeltabrechnung (CSV) sowie zur Bereitstellung der Daten an die Beschäftigten selbst.

2. Art der Verarbeitung

Erheben über die verschlüsselte Programmierschnittstelle der App, Speichern in einer Datenbank, Versionieren (anfügend), Auswerten (Summen, Prüfhinweise), Bereitstellen im Arbeitgeber-Bereich und in der App, Exportieren (PDF, CSV, JSON), Einschränken (Deaktivieren von Beschäftigten, Sperren von Geräten), Löschen (bei Kontolöschung).

3. Art der personenbezogenen Daten

- Stammdaten der Beschäftigten: Anzeigenname; optional Personalnummer, E-Mail-Adresse und vertragliche Wochenstunden, soweit vom Auftraggeber hinterlegt; Status (aktiv/inaktiv), Zeitpunkte der Registrierung, der letzten Aktivität und der Deaktivierung.
- Arbeitszeitdaten: Zeiteinträge mit Beginn, Ende, Art (Arbeit/Pause), Zeitzone, Quelle (Stempelung, manueller Eintrag, Arbeitgeber), Bemerkung sowie je Version Urheber (Beschäftigte/Beschäftigter, Arbeitgeber-Konto, System), Zeitpunkt der Änderung auf dem Gerät und auf dem Server, Begründung für manuelle Einträge, Korrekturen und Löschungen.
- Gerätedaten: pro Installation eine zufällige Gerätekennung, Gerätebezeichnung (z. B. „iPhone 15“), Plattform, App-Version, Zeitpunkte von Registrierung, letzter Nutzung und Sperrung; Zugangstoken ausschließlich als SHA-256-Hash.
- Registrierungscode: Code, optional vorgesehener Name der/des Beschäftigten und Notiz, Gültigkeit, Einlösezeitpunkt.
- Protokolldaten: Zeitstempel und IP-Adressen in den Versionen der Zeiteinträge und im Aktivitätsprotokoll des Arbeitgeber-Kontos (Anlegen, Ändern, Löschen von Beschäftigten, Codes und Zeiteinträgen, Exporte, Anmeldungen) sowie kurzzeitig in den Webserver-Protokollen.
- Abgeleitete Daten: Tages-, Wochen- und Monatssummen, Soll-Ist-Vergleich bei hinterlegten Wochenstunden, Prüfhinweise; Dokument-Prüfsummen (SHA-256) erzeugter Nachweise.
- Nicht verarbeitet werden: Standortdaten, Fotos, Kontakte, Bildschirminhalte, Gesundheitsdaten, Bankdaten, Daten nach Art. 9 oder 10 DSGVO.

4. Kategorien betroffener Personen

- Beschäftigte des Auftraggebers (Arbeitnehmerinnen und Arbeitnehmer, Auszubildende, geringfügig Beschäftigte, sonstige Mitarbeitende), die die App mit dem Arbeitgeber-Konto verbunden haben.
- Nutzerinnen und Nutzer des Arbeitgeber-Kontos (Inhaber und weitere Zugänge), soweit ihr Name und ihre Handlungen im Versionsverlauf der Zeiteinträge und im Aktivitätsprotokoll erscheinen. Die Konto- und Vertragsdaten dieser Personen verarbeitet der Auftragnehmer als eigener Verantwortlicher (siehe Datenschutzerklärung).

5. Ort der Verarbeitung

Rechenzentrum des Unterauftragsverarbeiters Hetzner Online GmbH in Deutschland; Verwaltung und Support durch den Auftragnehmer von Göttingen aus. Keine Verarbeitung außerhalb der Bundesrepublik Deutschland.

Anlage 2 - Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die Maßnahmen beziehen sich auf den vom Auftragnehmer verantworteten Anwendungsbetrieb. Maßnahmen zur physischen Sicherheit des Rechenzentrums (Zutrittskontrolle, Stromversorgung, Brandschutz, Datenträgervernichtung) erbringt der Unterauftragsverarbeiter Hetzner Online GmbH; dessen aktuelle TOM-Dokumentation und Prüfberichte stellt der Auftragnehmer auf Anfrage bereit.

1. Vertraulichkeit

- Zutrittskontrolle: Betrieb ausschließlich in zertifizierten Rechenzentren des Unterauftragsverarbeiters in Deutschland mit elektronischer Zutrittskontrolle, Protokollierung und Videoüberwachung; keine Auftragsdaten auf Datenträgern in Büroräumen des Auftragnehmers.
- Zugangskontrolle Server: Administrativer Zugriff ausschließlich über SSH mit personengebundenen Schlüsselpaaren; Passwort-Anmeldung deaktiviert; Zugriff auf die für den Betrieb zwingend erforderlichen Personen beschränkt; Firewall mit Freigabe nur der benötigten Dienste; Datenbank nur lokal erreichbar.
- Zugangskontrolle Anwendung: Passwörter der Arbeitgeber-Konten werden ausschließlich als Hash nach dem jeweils aktuellen PHP-Standardverfahren (bcrypt/Argon2) gespeichert; Mindestlänge 12 Zeichen; Sperre nach 5 Fehlversuchen für 15 Minuten; zusätzliche Drosselung je IP-Adresse; zeitlich befristete Links für E-Mail-Bestätigung und Passwort-Zurücksetzung, Reset-Token nur als Hash gespeichert; Sitzungen mit sicheren Cookies (HttpOnly, Secure, SameSite) und CSRF-Schutz.
- Zugangskontrolle App: Zugangstoken der Geräte werden mit 192 Bit Zufall erzeugt, nur einmal übertragen und serverseitig ausschließlich als SHA-256-Hash gespeichert; auf dem Gerät Ablage im geschützten Speicher des Betriebssystems (Keychain/Keystore); Token können je Gerät vom Auftraggeber gesperrt werden; Registrierungs_codes sind einmalig verwendbar und zeitlich befristet.
- Zugriffskontrolle: Rollen- und Berechtigungskonzept (Inhaber, Verwalter; Beschäftigte sehen nur eigene Daten); jede Datenbankabfrage ist auf das jeweilige Arbeitgeber-Konto eingeschränkt (mandantenbezogene Filterung); keine übergreifenden Auswertungen.
- Trennungskontrolle: Logische Trennung der Daten je Arbeitgeber-Konto über eindeutige Zuordnung jedes Datensatzes; getrennte Datenbanken für Produktion und Test; keine Produktivdaten in Entwicklungsumgebungen.
- Pseudonymisierung/Datensparsamkeit: Für die Erfassung genügen Anzeigenname und Zeiten; Personalnummer, E-Mail und Wochenstunden sind optional; keine Standort- oder Nutzungsdaten; IP-Adressen nur in Protokollen zur Missbrauchsabwehr.
- Verschlüsselung: Transportverschlüsselung aller Verbindungen (App, Arbeitgeber-Bereich, Website) ausschließlich über HTTPS/TLS mit aktuellen Protokollversionen und HSTS; E-Mail-Versand über TLS-gesicherte Verbindung zum Unterauftragsverarbeiter.

2. Integrität

- Eingabekontrolle: Zeiteinträge werden anfügend versioniert; jede Version speichert Urheber (Typ, Kennung, Name), Zeitpunkt auf dem Gerät und auf dem Server, App-Version, IP-Adresse und – bei Korrekturen und Löschungen – eine Pflichtbegründung. Versionen werden nie überschrieben oder gelöscht; eine Löschung ist eine neue Version mit Löschvermerk.
- Aktivitätsprotokoll: Handlungen im Arbeitgeber-Bereich (Anlegen, Ändern, Deaktivieren von Beschäftigten; Codes; Korrekturen; Exporte; Anmeldungen und Passwortänderungen) werden mit Konto, Zeitpunkt und IP-Adresse protokolliert und sind für den Auftraggeber einsehbar.
- Weitergabekontrolle: Keine Schnittstellen zu Dritten; Exporte nur durch angemeldete, berechtigte Konten; erzeugte Nachweise tragen eine SHA-256-Prüfsumme über die enthaltenen Versionen, mit der ein Ausdruck dem Versionsverlauf zugeordnet werden kann.
- Serverzeit als Referenz: Jeder Eintrag speichert Gerätezeit und Serverzeit; Abweichungen werden sichtbar gemacht, nicht stillschweigend korrigiert.
- Softwareintegrität: Versionsverwaltung des Quellcodes, getrennte Test- und Produktivumgebung,

automatisierte Tests vor Veröffentlichungen, zeitnahes Einspielen von Sicherheitsaktualisierungen für Betriebssystem, PHP und Abhängigkeiten.

3. Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung der Datenbank mit 31 Tagen Vorhaltung (rollierend), verschlüsselt abgelegt und zugriffsbeschränkt auf den Systemverwalter, gespeichert in Deutschland; regelmäßige Wiederherstellungstests.
- Offline-Fähigkeit der App: Erfassung funktioniert ohne Netzverbindung; Einträge werden lokal gespeichert und bei Verbindung nachgeliefert, sodass ein Serverausfall keinen Datenverlust bei der Erfassung verursacht.
- Rechenzentrum mit redundanter Stromversorgung, Klimatisierung und Brandschutz (Unterauftragsverarbeiter); Überwachung des Serverbetriebs; Begrenzung von Anfragegrößen und -raten gegen Überlastung.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management: benannter Datenschutzbeauftragter; Verzeichnis der Verarbeitungstätigkeiten; Dokumentation der TOM; Überprüfung mindestens jährlich und bei wesentlichen Änderungen.
- Incident-Response-Management: definierter Ablauf für Sicherheitsvorfälle (Erkennen, Eindämmen, Analysieren, Melden nach § 8, Nachbereiten); Protokollauswertung bei Verdachtsfällen.
- Datenschutzfreundliche Voreinstellungen: Minimaler Datenumfang in der Voreinstellung; keine Tracking-, Analyse- oder Werbedienste in App und Web; keine Drittanbieter-Ressourcen auf der Website.
- Auftragskontrolle: Schriftliche Verträge nach Art. 28 DSGVO mit allen Unterauftragsverarbeitern; regelmäßige Prüfung ihrer Zertifikate und Prüfberichte; Weisungen des Auftraggebers werden ausschließlich über die Funktionen des Dienstes oder in Textform entgegengenommen und dokumentiert.
- Löschkonzept: Registrierungscode verfallen nach eingestellter Gültigkeit; Bestätigungs- und Reset-Links nach Fristablauf; Webserver-Protokolle nach 14 Tagen; Auftragsdaten bei Kontolöschung unmittelbar aus den Produktivsystemen und spätestens nach 31 Tagen aus den Sicherungen; keine automatische Löschung von Zeiteinträgen innerhalb der zweijährigen gesetzlichen Mindestaufbewahrung.

Anlage 3 - Genehmigte Unterauftragsverarbeiter

Stand dieser Anlage: Fassung dieses Vertrags. Änderungen werden nach § 6 mit 30 Tagen Vorankündigung mitgeteilt.

- Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland – Leistung: Bereitstellung und Betrieb der Serverinfrastruktur (Rechenzentrum, Hardware, Netzanbindung) für Anwendung, Datenbank und Datensicherungen. Ort der Verarbeitung: Deutschland. Es besteht ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO zwischen dem Auftragnehmer und Hetzner Online GmbH.
- ALL-INKL.COM – Neue Medien Münnich, Inhaber René Münnich, Hauptstraße 68, 02742 Friedersdorf, Deutschland – Leistung: Versand der vom Dienst erzeugten E-Mails (E-Mail-Bestätigung, Passwort-Zurücksetzung, Einladungscodes an Beschäftigte). Verarbeitete Daten: E-Mail-Adresse der Empfängerin/des Empfängers, Name, Inhalt der jeweiligen Nachricht. Ort der Verarbeitung: Deutschland. Es besteht ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO zwischen dem Auftragnehmer und ALL-INKL.COM.

Weitere Unterauftragsverarbeiter, insbesondere Zahlungsdienstleister für kostenpflichtige Tarife, werden vor ihrem Einsatz nach § 6 angekündigt und in diese Anlage aufgenommen. Der Bezug der App über den Apple App Store oder Google Play ist kein Unterauftragsverhältnis; die Store-Betreiber

erhalten keine Auftragsdaten.

Summary in English (non-binding)

This Data Processing Agreement under Art. 28 GDPR is concluded between the employer who registers an employer account for the Zeitrachweis service (the controller) and Desatec Systems GmbH, Göttingen, Germany (the processor). It is accepted electronically by ticking the corresponding checkbox at sign-up; the timestamp and version accepted are stored with the employer account. The processor stores, versions and reports working-time records of the employer's staff solely on the employer's documented instructions, exclusively on servers in Germany, with no transfer to third countries. Data categories are limited to display name, optional personnel number, time entries (start, end, type), reasons for corrections, device name, app version, timestamps and IP addresses in audit logs. Technical and organisational measures include TLS-only transport, password hashing, access tokens stored only as SHA-256 hashes, append-only versioning with a full audit trail, role-based access, daily encrypted backups kept for 31 days, hosting at Hetzner in Germany and SSH-key-only administration. Approved sub-processors are Hetzner Online GmbH (hosting) and ALL-INKL.COM – Neue Medien Münnich (e-mail delivery); changes are announced 30 days in advance with a right to object. The processor supports the controller with data-subject requests and with Art. 32–36 GDPR obligations, reports personal data breaches without undue delay and at the latest within 48 hours, allows audits with prior notice, and deletes all data after the contract ends once the controller has exported it; statutory retention duties (at least two years under German working-time and minimum-wage law) remain the controller's responsibility. German law applies, place of jurisdiction is Göttingen, and only the German text is legally binding.