Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Version 4.0

Vereinbarung zwischen dem/der

Verantwortlichen – nachstehend „Kunde“ genannt, der dieser Vereinbarung zustimmt

und dem

Auftragsverarbeiter – TimeTrack GmbH, Paulanergasse 13/8, 1040 Wien, Österreich – nachstehend „Anbieter“ genannt.

§ 1. Gegenstand und Dauer der Vereinbarung

(1) Gegenstand der Vereinbarung ist der Austausch von Daten iZm der Nutzung der Zeiterfassungssoftware TimeTrack.

(2) Die Dauer dieser Vereinbarung entspricht der Dauer des Vertragsverhältnisses zwischen dem Kunden und dem Anbieter.

§ 2. Konkretisierung des Vereinbarungsinhalts

(1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Land, das nicht der Europäischen Union oder dem Europäischen Wirtschaftsraum angehört, bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau des Drittlandes gemäß § 6 wird entweder durch die Europäische Kommission (Artikel 45 Absatz 3 DS-GVO) oder einen anerkannten Zertifizierungs-Mechanismus festgestellt (Artikel 46 Absatz 2 Punkt f in Verbindung mit Artikel 42 DS-GVO).

(2) Die Arten der personenbezogenen Daten, die verarbeitet werden, sind präzise in Anhang 1 dieser Vereinbarung definiert.

(3) Die Kategorien der betroffenen Personen sind präzise in Anhang 1 dieser Vereinbarung definiert.

§ 3. Technisch-organisatorische Maßnahmen

(1) Der Anbieter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Kunden zur Prüfung zu übergeben. Bei Akzeptanz durch den Kunden werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Kunden einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Anbieter hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. 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 DS-GVO zu berücksichtigen [Näheres dazu im Anhang 2].

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

§ 4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Anbieter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Anbieter wendet, wird der Anbieter dieses Ersuchen unverzüglich an den Kunden weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Kunden unmittelbar durch den Anbieter sicherzustellen.

§ 5. Pflichten des Kunden

(1) Der Kunde ist Besitzer der Kundendaten und Inhaber aller Rechte betreffend diesen Kundendaten.

(2) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung der betroffenen Personen, sowie Aufrechterhaltung der Rechte der betroffenen Personen verantwortlich.

(3) Der Kunde ist dafür verantwortlich, Aufzeichnungen in Bezug auf nationale Gesetze, oder Gesetze von Mitgliedstaaten, zu führen. Der Anbieter ist nicht haftbar

für die Vollständigkeit der Daten oder die Aufrechterhaltung von Regulationen und Gesetzen.

§ 6. Qualitätssicherung und sonstige Pflichten des Anbieters

Der Anbieter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Anbieter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Anbieter und jede dem Anbieter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Kunden verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Näheres dazu in Anlage 1].
- Der Kunde und der Anbieter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Kunden über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Anbieter ermittelt.
- Soweit der Kunde seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Anbieter ausgesetzt ist, hat ihn der Anbieter nach besten Kräften zu unterstützen.
- Der Anbieter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Kunden im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

§ 7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Anbieter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung

und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Anbieter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Kunden auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Anbieter darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Kunden beauftragen. Der Kunde stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu:

Unternehmen	Adresse	Leitung
Digital Ocean	101 Avenue of the Americas, 10th Floor, New York, NY, 10013, United States (Data Center in Frankfurt, Deutschland)	Hosting Provider,
Stripe	1 Grand Canal Street Lower, Grand Canal Dock, D02 H210, Dublin, Ireland	Zahlungsanbieter
AWS-Amazon Web Services	5 rue Plaetis, L-2338, Luxemburg, Luxemburg	E-mail Versand
Droptop GmbH/Linevast	Am Grashorn 8, 14548 Schwielowsee, Deutschland	Hosting Homepage und E-Mails

Der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Anbieter eine solche Auslagerung auf Unterauftragnehmer dem Kunden eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Kunde nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Anbieter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

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

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Anbieter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Kunden (mind. Textform);

§ 8. Kontrollrechte des Auftraggebers

(1) Der Kunde hat das Recht, im Vernehmen mit dem Anbieter Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Anbieter in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Anbieter stellt sicher, dass sich der Kunde von der Einhaltung der Pflichten des Anbieters nach Art. 28 DS-GVO überzeugen kann. Der Anbieter verpflichtet sich, dem Kunden auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Für die Ermöglichung von Kontrollen durch den Kunden kann der Anbieter einen Vergütungsanspruch geltend machen.

§ 9. Mitteilung bei Verstößen des Anbieters

(1) Der Anbieter unterstützt den Kunden bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Kunden zu melden;
- die Verpflichtung, dem Kunden im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- die Unterstützung des Kunden für dessen Datenschutz-Folgenabschätzung;
- die Unterstützung des Kunden im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten, oder nicht auf ein Fehlverhalten des Anbieters zurückzuführen sind, kann der Anbieter eine Vergütung beanspruchen.

§ 10. Weisungsbefugnis des Auftraggebers

(1) Der Kunde muss alle Instruktionen in Textform mitteilen.

(2) Der Anbieter hat den Kunden unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Anbieter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

§ 11. Kopieren, Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Bis zu 30 Tagen nach der Kündigung dieser Vereinbarung kann der Kunde verlangen, seine Daten retourniert zu bekommen (in dem Ausmaß, das noch nicht vom Kunden gelöscht wurde). Die Daten werden in einem allgemein verwendeten und offenen Dateiformat bereitgestellt. Auf ausdrückliches Verlanden des Kunden kann der Anbieter sämtliche Kundendaten (einschließlich Kopien) in seinem Besitz oder unter seiner Kontrolle löschen, es sei denn der Anbieter untersteht einem Gesetz der Europäischen Union oder eines Mitgliedstaates zur Aufbewahrung eines Teils oder der gesamten Kundendaten. Das Protokoll der Zerstörung der Löschung wird nach Aufforderung bereitgestellt.

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

§ 12. Gültigkeit dieser Vereinbarung

Die Annahme dieser Vereinbarung darf nur durch vertretungsberechtigte Personen des Kunden erfolgen.

Diese Vereinbarung ist ab elektronischer Bestätigung gültig. Diese Vereinbarung orientiert sich an der DS-GVO und ist ab 25. Mai 2018 gültig.

Anlage 1 – Datenverarbeitung

Kategorien von betroffenen Personen

Mitarbeiter, Unterbeauftragte, Vertreter, Kunden und andere betroffene Personen auf Seiten des Kunden, die Zugriff auf TimeTrack-Systeme haben und diese nutzen sollen, werden gesamt als “Nutzer” genannt.

Arten personenbezogener Daten

Kategorie	Daten
Name	Vorname *, Nachname *
Nutzer Identifikation	Nutzername *
Elektronische Identifikationsdaten	IP Adresse *
Kontaktinformationen	E-Mail-Adresse*, Telefonnummer, Kontaktadresse und Land
Lokalisierungsdaten	GeoLocation/GPS Daten
vom Kunden eingegebenen Daten	Dies deckt alle anderen persönlichen Daten ab, die der Kunde in die benutzerdefinierten Felder eintragen kann.

Daten markiert mit “*” sind zwingend notwendig. Alle anderen Daten sind optional.

Anlage 2 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zugangskontrolle
  - Keine unbefugte Systembenutzung
  - Passwortrichtlinien
  - Private/Public Keys
- Zugriffskontrolle
  - Kein unbefugtes Lesen, Kopieren, Verändern oder Löschen von Daten
  - Berechtigungskonzepte
  - Protokollierung von Zugriffen und Events
- Trennungskontrolle
  - Trennung von Kundenaccounts in den Datenbanken
  - Getrennte Umgebungen für Entwicklung, Staging und Production

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  - Kein unerlaubtes Lesen, Kopieren, Ändern oder Löschen der Daten
- Eingabekontrolle
  - Überprüfung, ob, von wem und zu welchem Zeitpunkt persönliche Daten vom Anbieter in das Datenverarbeitungssystem eingetragen wurden.
  - Zugangsprotokoll
  - Accountprotokoll, wie z.B. Request-Logs
  - Nutzerrechte und -rollen in der Software des Anbieters
- Verschlüsselung
  - Alle Requests
  - Verbindungen
  - Transfer
- Einhaltung beim Mitarbeiter
  - Datenschutz-Training mit regelmäßigen Überprüfungen
  - Verpflichtungserklärung zum Datengeheimnis

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zertifizierte, skalierbare Datenzentren in EU
- Externe Backup Bestimmungen
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
- Stresstests
- Notfallwiederherstellungsplan