Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

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) Diese Vereinbarung (in der Folge „Vereinbarung“) regelt die Verarbeitung von personenbezogenen Daten (in der Folge „Daten“) durch den Anbieter im Auftrag des Kunden (in der Folge „Auftragsverarbeitung“).

(2) In der Vereinbarung vorkommende Begriffe (z.B. betroffene Person, Dritter, Drittland usw.) sind im Sinne der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (im Folgenden „DSGVO“) auszulegen, es sei denn, die in der Vereinbarung verwendeten Begriffe sind ausdrücklich definiert.

(3) Der Gegenstand der jeweiligen vom Anbieter durchgeführten Auftragsverarbeitung ist in **Anhang I** zur Vereinbarung geregelt. Die Anhänge zur Vereinbarung sind integraler Bestandteil der Vereinbarung. Bei Widerspruch oder Unvereinbarkeit gehen Bestimmungen in den Anhängen den Bestimmungen im Hauptteil der Vereinbarung vor. Nicht Gegenstand der Vereinbarung ist die Regelung der wirtschaftlichen und rechtlichen Konditionen sowie eine genaue technische oder fachmännische Beschreibung der zu erbringenden Dienstleistungen des Anbieters. Die Dauer dieser Vereinbarung entspricht der Dauer des Vertragsverhältnisses zwischen dem Kunden und dem Anbieter.

(4) Die Anhänge zur Vereinbarung beschreiben Zweck und die Art der Auftragsverarbeitung, die vom Auftragsverarbeiter verarbeiteten Kategorien betroffener Personen und die Arten verarbeiteter Daten sowie die für die Auftragsverarbeitung vereinbarten technischen und organisatorischen Maßnahmen.

§ 2. Konkretisierung des Vereinbarungsinhalts

Die Erbringung der vertraglich vereinbarten Datenverarbeitung erfolgt grundsätzlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Eine Verarbeitung personenbezogener Daten in einem Drittland oder ein Zugriff auf personenbezogene Daten aus einem Drittland darf nur erfolgen, soweit der Kunde hierzu vorab allgemein oder im Einzelfall seine Zustimmung erteilt hat und die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Der Anbieter stellt in diesem Fall

sicher, dass für die betreffende Verarbeitung ein angemessenes Datenschutzniveau gewährleistet ist, insbesondere durch einen Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO oder durch geeignete Garantien gemäß Art. 46 DSGVO.

§ 3. Technisch-organisatorische Maßnahmen

(1) Der Anbieter setzt die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen um. Diese Maßnahmen gelten als vereinbart und sind Grundlage der Auftragsverarbeitung. Der Anbieter ist berechtigt, die technischen und organisatorischen Maßnahmen an technische und organisatorische Weiterentwicklungen anzupassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen wird der Anbieter dem Kunden auf Anfrage darlegen.

(2) Der Anbieter hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO 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.

(3) Ist der Kunde auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Informationen oder Auskünfte zur Verarbeitung von Daten dieser Person zu erteilen oder die Rechte von betroffenen Personen nach Kapitel III

(Artt. 12 bis 23) der DSGVO zu gewährleisten, wird der Anbieter den Kunden angesichts der Art der Verarbeitung bei der Erfüllung dieser Pflichten nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen entsprechend Art. 28 Abs. 3 lit. e DSGVO unterstützen.

§ 5. Pflichten des Kunden

(1) Der Kunde ist Verantwortlicher im Sinne der DSGVO für die im Rahmen dieser Vereinbarung verarbeiteten personenbezogenen Daten.

(2) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung, die Erteilung von Weisungen sowie die Wahrung der Rechte der betroffenen Personen verantwortlich.

(3) Der Kunde ist dafür verantwortlich, dass die Verarbeitung personenbezogener Daten auf einer gültigen Rechtsgrundlage beruht und gesetzliche Informationspflichten erfüllt werden.

(4) Der Anbieter prüft die vom Kunden übermittelten Daten grundsätzlich nicht auf ihre materielle Rechtmäßigkeit, Richtigkeit oder Vollständigkeit.

§ 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 DSGVO; 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 2].
- 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.

Soweit eine Datenverarbeitung durch einen Unteranbieter nach diesem Vertrag zulässigerweise außerhalb eines Mitgliedstaats der Europäischen Union oder außerhalb eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum stattfindet, stellt der Anbieter sicher, dass diese nach aktuellen Standards derart hoch verschlüsselt werden, dass diese mit dem Einsatz vernünftiger technischer Mittel durch andere Personen als dem Anbieter nicht gelesen werden können.

(2) Der Kunde erteilt dem Anbieter die allgemeine Genehmigung, die in dieser Vereinbarung und ihren Anhängen genannten Unterauftragsverarbeiter einzusetzen. Der Kunde stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

Allgemein eingesetzte Unterauftragsverarbeiter:

Name und Sitz des Unterauftragsverarbeiters	***Ort der Datenverarbeitung***	***Zweck der Verarbeitung:***
DigitalOcean, LLC	Rechenzentrumsstandort:	Hosting-Infrastruktur für den Betrieb der Anwendung auf einem

101 6th Ave / 101 Avenue of the Americas, New York, NY 10013, USA	Frankfurt am Main, Deutschland, DigitalOcean-Region FRA1	ISO/IEC 27001-zertifizierten Virtual Private Server (VPS). Die Datenübertragung erfolgt verschlüsselt. Gespeicherte Daten werden verschlüsselt abgelegt[1].
Droptop GmbH / Linevast Am Grashorn 8, 14548 Schwielowsee OT Geltow, Deutschland	Rechenzentrumstandort: Schwielowsee, Deutschland	Hosting und Bereitstellung von E-Mail-Diensten
Zoho Corporation B.V. Beneluxlaan 4B, 3527 HT Utrecht, Niederlande	Rechenzentrumstandorte: Amsterdam, Niederlande und Dublin, Irland	CRM-System zur Verwaltung von Kunden-, Interessenten- und Geschäftskontaktdaten
Dropbox International Unlimited Company One Park Place Upper Hatch Street Dublin 2 D02 FD79 Irland	Rechenzentrumstandort: Dublin, Irland	Dateiablage, Datenaustausch und/oder Backup-Speicherung. Die Datenübertragung erfolgt verschlüsselt. Gespeicherte Daten werden verschlüsselt abgelegt[2].

Die folgenden Unterauftragsverarbeiter werden nur eingesetzt, soweit die jeweilige Funktion durch den Kunden genutzt und nicht abgewählt wurde. Bestehende **Opt-out- oder Alternativmöglichkeiten** sind vom Kunden ausdrücklich gegenüber dem Anbieter in Textform geltend zu machen:

---

[1] Die auf den DigitalOcean-Servern gespeicherten Daten werden verschlüsselt abgelegt. Die Verschlüsselung erfolgt mittels **AES-256-CBC** bzw. vergleichbarer starker Verschlüsselungsverfahren. Die hierfür erforderlichen Entschlüsselungsschlüssel werden ausschließlich von der TimeTrack GmbH verwaltet. DigitalOcean hat keinen Zugriff auf diese Schlüssel; eine Entschlüsselung der gespeicherten Daten ist daher nur durch die TimeTrack GmbH möglich. Die Wiederherstellbarkeit der verschlüsselten Daten wird regelmäßig getestet.

[2] Die Datenablage auf den Dropbox Servern erfolgt unter Anwendung von **AES-256-CBC**-Verschlüsselung. Zugang zum 256-bit Schlüssel hat nur TimeTrack GmbH. Eine Entschlüsselung der gespeicherten Daten nur seitens TimeTrack GmbH möglich.

Name und Sitz des Unterauftragsverarbeiters	***Ort der Datenverarbeitung***	***Zweck der Verarbeitung:***	***Opt-out/ Alternative***
Stripe Payments Europe, Limited One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Ireland	Rechenzentrumstandort: Dublin, Ireland	Zahlungsdienstleister für Kreditkarten- und Online-Zahlungen. Bei Zahlung per Rechnung wird Stripe nicht verwendet.	Opt-out durch Zahlung per Rechnung
Amazon Web Services EMEA S.à r.l. 38 Avenue John F. Kennedy, L-1855 Luxembourg	Rechenzentrumstandorte: Deutschland, AWS Region Europe (Frankfurt), eu-central-1 Irland, AWS Region Europe (Ireland), eu-west-1	Versand transaktionaler System-E-Mails, z. B. Systembenachrichtigungen, Workflow-E-Mails, Genehmigungsanfragen, Erinnerungen und technische Systemmeldungen. Die Nutzung dient ausschließlich der zuverlässigen technischen Zustellung transaktionaler E-Mails, insbesondere der Sicherstellung einer hohen Zustellbarkeit, einer stabilen Versand-Infrastruktur sowie ausreichender Versandkapazitäten bei hohem E-Mail-Aufkommen. AWS SES dient nicht der dauerhaften Speicherung, Analyse oder Auswertung von Kundendaten.	Optional: Nutzung eines kundeneigenen SMTP-Servers, sofern vereinbart und konfiguriert
Functional Software, Inc. d/b/a Sentry 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Rechenzentrumstandort: Frankfurt, Deutschland	Reines Software-Crash-Reporting zur technischen Fehleranalyse, Stabilitätsüberwachung und Fehlerbehebung. Der Zweck der Verarbeitung besteht ausschließlich darin, Softwarefehler frühzeitig zu erkennen, insbesondere auch solche, die nur bei bestimmten kundenspezifischen Einstellungen oder Konstellationen auftreten, und dadurch eine schnelle Fehlerbehebung sowie eine	Optional deaktivierbar, soweit schriftlich vereinbart

		hohe Stabilität und Qualität der Software sicherzustellen. Es werden keine Performance-, Tracking- oder Analytics-Daten an Sentry übermittelt. Eine planmäßige Übermittlung fachlicher Kundendaten findet nicht statt. Insbesondere werden Namen, E-Mail-Adressen, Inhalte von Zeiterfassungen, Abwesenheitsgründe, Kommentare, Personalnummern, Standortdaten, Authentifizierungsdaten sowie sonstige fachliche Inhaltsdaten vor der Übermittlung, soweit technisch möglich, ausgeschlossen, maskiert oder herausgefiltert. Die Übermittlung wird durch SDK-seitiges Scrubbing sowie zusätzliche serverseitige Filterregeln auf das technisch erforderliche Mindestmaß reduziert.	

Der Anbieter wird den Kunden über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern rechtzeitig, mindestens 14 Tage vor deren Einsatz, in Textform informieren. Der Kunde kann gegen eine solche Änderung innerhalb von 10 Tagen ab Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform Widerspruch einlegen.

(3) Der Anbieter wird mit jedem Unterauftragsverarbeiter eine Vereinbarung abschließen, die diesem mindestens diejenigen Datenschutzpflichten auferlegt, die nach Art. 28 DSGVO erforderlich sind und die für die vom Unterauftragsverarbeiter übernommenen Verarbeitungstätigkeiten gelten. Der Anbieter bleibt gegenüber dem Kunden für die Erfüllung der datenschutzrechtlichen Verpflichtungen des Unterauftragsverarbeiters verantwortlich.

(4) Soweit ein Unterauftragsverarbeiter oder ein sonstiger vom Anbieter eingesetzter Dienstleister personenbezogene Daten außerhalb der EU oder des EWR verarbeitet oder aus einem Drittland auf solche Daten zugreift, stellt der Anbieter sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden.

(5) Eine weitere Beauftragung von Unterauftragsverarbeitern durch einen Unterauftragsverarbeiter bedarf der vorherigen allgemeinen oder gesonderten Zustimmung des Kunden.

(6) **Optionale Integrationen / Schnittstellen**:
Auf Wunsch und nach entsprechender Weisung des Kunden können weitere Integrationen und Schnittstellen zu Dritt- bzw. Partnersystemen eingerichtet werden. Diese Integrationen dienen insbesondere dem Austausch von Stamm-, Zeit-, Abwesenheits-, Projekt- oder Abrechnungsdaten mit vom Kunden eingesetzten Systemen.

Mögliche Integrationen sind beispielsweise Schnittstellen zu DATEV, Lexware Office/Lexoffice, Personio, Addison (eAU) sowie zu weiteren Lohn-, HR-, Buchhaltungs- oder ERP-Systemen.

Eine Datenübermittlung an solche Systeme erfolgt nur, soweit die jeweilige Integration durch den Kunden beauftragt, aktiviert oder technisch konfiguriert wurde und für den vereinbarten Zweck erforderlich ist.

§ 8. Kontrollrechte des Auftraggebers

(1) Der Kunde hat das Recht, nach angemessener vorheriger Ankündigung Überprüfungen selbst oder durch einen im Einzelfall zu benennenden, zur Verschwiegenheit verpflichteten Prüfer durchführen zu lassen. Dabei sind die berechtigten Betriebs- und Geschäftsgeheimnisinteressen des Anbieters angemessen zu berücksichtigen.

(2) Der Anbieter stellt sicher, dass sich der Kunde von der Einhaltung der Pflichten des Anbieters nach Art. 28 DSGVO 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) Soweit Kontrollen des Kunden über die Bereitstellung üblicher Nachweise, Auskünfte und Unterlagen hinausgehen oder Vor-Ort-Prüfungen verursachen, kann der Anbieter hierfür einen angemessenen, vorher angekündigten Aufwand in Rechnung stellen.

§ 9. Mitteilung bei Verstößen des Anbieters

(1) Der Anbieter unterstützt den Kunden bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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 Weisungen 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) Nach Beendigung der Leistungserbringung wird der Anbieter auf Weisung des Kunden die personenbezogenen Daten entweder löschen oder in einem gängigen maschinenlesbaren Format herausgeben, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Gesetzlich aufzubewahrende Daten werden nach Ablauf der Aufbewahrungspflichten gelöscht.

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

§ 12. Gültigkeit dieser Vereinbarung

Diese Vereinbarung ist integraler Bestandteil des zwischen den Parteien bestehenden Vertragsverhältnisses und tritt mit Abschluss des Hauptvertrags oder mit gesonderter Annahme durch den Kunden in Kraft.

Anlage 1 – Datenverarbeitung

1. Gegenstand, Zweck und Art der Auftragsverarbeitung

Gegenstand der Auftragsverarbeitung ist die Bereitstellung, der Betrieb und die technische Unterstützung der Software TimeTrack. Zweck der Verarbeitung ist die Durchführung der Zeiterfassung und Zeitplanung für Mitarbeiter des Verantwortlichen. Die Art der Verarbeitung umfasst insbesondere das Erfassen, Speichern, Organisieren, Bereitstellen und sonstige Verarbeiten personenbezogener Daten auf den vom Auftragsverarbeiter betriebenen Systemen.

2. Kategorien der 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 gemeinsam als “Nutzer” genannt.

3. Arten personenbezogener Daten

Kategorie	Daten
Name	Vorname*, Nachname*
Nutzeridentifikation	Nutzername*, Terminalbezogene Identifikationsdaten, Zutrittsbezogene Identifikationsdaten
Elektronische Identifikationsdaten	IP-Adresse*
Persönliche Details	Geschlecht, Geburtsdatum, Geburtsort, Geburtsname
Kontaktinformationen	E-Mail-Adresse*, Telefonnummer, Kontaktadresse und Land
Lokalisierungsdaten	Standortdaten (GPS-Daten)
Sozialversicherung	Sozialversicherungsnummer
Anstellungsinformationen	Rolle, Eintrittsdatum, Austrittsdatum, Personalnummer, Arbeitszeitaufzeichnungen, Abwesenheitsgrund.

Organisationsdaten	Abteilungszugehörigkeit, Abteilungsfunktion, Projekte, Projektstunden, Projektausgaben
Sonstige vom Kunden eingegebene personenbezogene Daten	Hierunter fallen sonstige personenbezogene Daten, die der Kunde in benutzerdefinierten Feldern erfasst.

Daten markiert mit “*” sind zwingend notwendig. Alle weiteren Daten sind optional und hängen von den jeweils gewählten bzw. freigeschalteten Softwarefunktionen ab.

Anlage 2 – Technisch-organisatorische Maßnahmen

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

- **Zutrittskontrolle**
  - Kein unerlaubter Zutritt zu den Büroräumlichkeiten;
  - Der Zutritt wird ausschließlich aktiv angestellten Mitarbeitern gewährt;
  - Bürobesucher werden immer von Mitarbeitern begleitet.
  - Videoüberwachung des Eingangsbereichs.
- **Zugangskontrolle**
  - Keine unbefugte Systembenutzung; der Zugang wird durch Authentifizierungsmechanismen eingeschränkt;
  - Passwortrichtlinien;
  - Absperrmechanismen für Arbeitsplätze („clean desk policy“ sowie automatische Sperrung nach einer Inaktivität von bestimmter Dauer);
  - Private/Public Keys für alle Serverzugänge.
- **Zugriffskontrolle**
  - Kein unbefugtes Lesen, Kopieren, Verändern oder Löschen von Daten. Alle Tätigkeiten werden aufgezeichnet und überprüft;
  - Berechtigungskonzepte: Mitarbeiter erhalten eingeschränkten Zugang gemäß ihrer Tätigkeitsbeschreibung;
  - Protokollierung von Zugriffen und Tätigkeiten (Einloggen, Ausloggen, Veränderungen, Löschungen).
- **Trennungskontrolle**
  - Trennung von Kundenkonten in den Datenbanken;
  - Trennung von Kundendaten innerhalb eines Kontos in Datenbanken;
  - Getrennte Umgebungen für *Development*, *Staging* und *Production*.
- **Pseudonymisierung**
  - Pseudonymisierung der Nutzerdaten wo möglich

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

- **Weitergabekontrolle**
  - Datenübermittlungen und Zugriffe werden protokolliert, soweit dies technisch vorgesehen und datenschutzrechtlich zulässig ist;
  - Firewall zum Schutz des Datenverkehrs und der Endgeräte im Netzwerk.
- **Eingabekontrolle**
  - Aufzeichnungen, ob, von wem und zu welchem Zeitpunkt persönliche Daten in das Datenverarbeitungssystem eingetragen oder geändert wurden;
  - Zugangsprotokoll der Zugangsversuche;
  - Kontoprotokolle, z. B. Anfrageprotokolle
  - Nutzerrechte und -rollen in der Software des Anbieters, um unbefugte Manipulation zu verhindern.
- **Verschlüsselung**
  - *at rest*: LUKS2 Verschlüsselung mit aes-xts-plain64 (Schlüssellänge 512 bits)

    - *backups*: aes-256-cbc Verschlüsselung auf dem Anwendungserver (separate Platte)
- **Einhaltung beim Mitarbeiter**
    - Datenschutz-Training mit regelmäßigen Überprüfungen
    - Verpflichtungserklärung zum Datengeheimnis
    - IT-Sicherheitsbestimmungen
    - Onboarding-/Offboarding-Prozesse für Mitarbeiter

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

- ISO27001 Zertifiziertes Datenzentrum in Frankfurt, Deutschland, Selbst verwaltete VPS
- Externe Backup-Regelungen
- Maßnahmen zur raschen Wiederherstellbarkeit gemäß Art. 32 Abs. 1 lit. c DSGVO, einschließlich eines Notfallwiederherstellungsplans. Täglich vollständige Datenbank-Server Sicherung, Wiederherstellung der einzelnen Kunden-Datenbanken möglich (RPO bis zu 24h, RTO: bis zu 24h).

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

- **Datenschutz-Management** einschließlich regelmäßiger Mitarbeiter-Schulungen: Der Anbieter stellt seinen Mitarbeitern alle erforderlichen Informationen und Mittel zur Umsetzung von Maßnahmen zur Verfügung, um eine datenschutzkonforme Gestaltung der Technik und Organisation sicherzustellen. Alle Mitarbeiter des Anbieters sind verpflichtet, die Sicherheit von Informationen und Informationssystemen, auf die sie Zugriff haben, zu wahren und aktiv zu fördern.
- **Schwachstellenanalysen**: Der Anbieter führt regelmäßige Schwachstellenanalysen und Sicherheitsüberprüfungen der eingesetzten Systeme und Webanwendungen durch. Die Prüfungen orientieren sich an anerkannten Standards und Best Practices, insbesondere am OWASP Web Security Testing Guide (WSTG), an den OWASP Top 10 sowie am NIST SP 800-115.
- **Incident-Response-Management:** Ziel ist die Wiederherstellung des definierten Betriebszustands eines IT-Services für den Kunden im Rahmen der vereinbarten Servicequalität, um die Minimierung der Beeinträchtigung der Geschäftsprozesse zu erreichen. Sobald das Incident Management die Einhaltung der Service Levels gefährdet sieht, erfolgt eine Eskalation. Innerhalb der IT-Organisation bildet das Incident Management die Schnittstelle zu anderen IT-Servicebereichen (z. B. *Problem, Change, Configuration, Release . . .).* Neben Störungen werden auch andere Kundenanfragen (*Service Requests*) der Anwender erfasst, erste Hilfestellung geleistet und gegebenenfalls die weitere Bearbeitung in den nachgelagerten Supporteinheiten koordiniert.
- **Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DSGVO): In der Planungsphase zur

Beschaffung einer neuen oder zur Änderung einer bestehenden Datenanwendung wird ein unternehmensinterner Anforderungskatalog erstellt. Auf Grundlage des Anforderungskatalogs wird im Vorfeld die Rechtmäßigkeit der vorgesehenen Datenverarbeitung intern geprüft. Unter den Gesichtspunkten der Datenvermeidung und einer Datensparsamkeit werden die Anforderungen für eine datenschutzkonforme Gestaltung der Datenanwendung sowie die technischen und organisatorischen Voraussetzungen definiert.

- **Auftragskontrolle der Unterauftragsverhältnisse**: Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Verantwortlichen, z.B.: strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), vorherige Prüfung, Nachkontrollen.