Vertrag über die Verarbeitung von Daten im Auftrag

zwischen	und
TempoBill GmbH	**Mustermann GmbH**
Im Mediapark 5	**Max Mustermann**
50670 Köln	**Musterstraße 1**
Telefon: +49 (0)221 999 8988-0	**12345 Musterort**
EMail: office@tempobill.de	**Telefon: +49 (1234) 56789-0**
Web: www.tempobill.de	**EMail: max@mustermann.de**
nachfolgend Auftragnehmer genannt	nachfolgend Verantwortlicher genannt

Die Parteien - Auftragnehmer und Auftraggeber - schließen einen Vertrag zur Verarbeitung von Daten im Zusammenhang mit der Nutzung der Software "Zeiterfassung.APP" auf Mietbasis und vereinbaren folgendes:

§ 1 Präambel

(1) Der Verantwortliche beauftragt den Auftragnehmer mit der Verarbeitung personenbezogener Daten unter Beachtung nachfolgender Regelungen.

(2) Im Rahmen der Leistungserbringung nach dem Hauptvertrag ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten des Verantwortlichen umgeht. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Daten des Verantwortlichen zur Durchführung des Hauptvertrags.

§ 2 Gegenstand des Auftrags und Konkretisierung des Auftragsinhalts

(1) Bei dem Hauptvertrag handelt es sich um Software-Mietvertrag für die Zeiterfassungs-Software Zeiterfassung.APP vom 08.11.2019, auf den hier verwiesen wird.

(2) Der Auftrag umfasst ausschließlich die in Anhang 1 beschriebene Dienstleistung (= Gegenstand der Auftragstätigkeit). Art und Zweck der vorgesehenen Verarbeitung personenbezogener Daten sowie die Art der Daten und die Kategorien betroffener Personen ergeben sich aus Anhang 1 dieser Vereinbarung.

(3) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Eine – auch nur teilweise - Verlagerung der Dienstleistung oder eine Auftragserfüllung außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums bedarf ebenfalls der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der Art 44 ff. DSGVO erfüllt sind.

(4) Die Auftragserledigung durch den Auftragnehmer in Privatwohnungen erfolgt nur mit vorheriger schriftlicher Zustimmung durch den Verantwortlichen nach Vorlage eines Sicherheitskonzepts. Grundsätzlich ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen; dies gilt auch für die Maßnahmen nach Art. 32 DSGVO.

§ 3 Pflichten des Verantwortlichen

(1) Der Verantwortliche ist für die Beurteilung der datenschutzrechtlichen Zulässigkeit der Auftragsverarbeitung gemäß Art. 6 Abs. 1 DSGVO, der Einhaltung von gesetzlichen Bestimmungen des Datenschutzes sowie für die Wahrung der Rechte der Betroffenen gemäß Art. 12 bis 22 DSGVO verantwortlich. Der Auftragnehmer ist verpflichtet, alle Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiter zu leiten.

(2) Der Verantwortliche erteilt alle Weisungen schriftlich oder in Textform. Er hat das Recht, dem Auftragnehmer Weisungen über Art, Umfang und Verfahren der Datenverarbeitung oder diesbezügliche Änderungen zu erteilen.

(3) Der Verantwortliche informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Verantwortliche ist verpflichtet, die für die Leistungserbringung erforderlichen Angaben, Daten, Schriftstücke und Datenbestände dem Auftragnehmer rechtzeitig in der im Einzelnen vereinbarten Form zur Verfügung zu stellen.

(5) Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertrages bestehen.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(2) Der Auftragnehmer ist für die Beurteilung der datenschutzrechtlichen Zulässigkeit der Auftragsverarbeitung, die Einhaltung von gesetzlichen Bestimmungen im Rahmen seiner gesetzlichen Verantwortung des Datenschutzes sowie für die Unterstützung der Wahrung der Rechte der Betroffenen mitverantwortlich.

(3) Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer einen Datenschutzbeauftragten sowie wenn nötig einen Vertreter im Sinne des Art. 27 DSGVO. Als Datenschutzbeauftragter wird eine Person bestellt, die die gesetzlich vorgeschriebenen Voraussetzungen erfüllt. Die Kontaktdaten des Datenschutzbeauftragten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(4) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer 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 dokumentiert sämtliche Weisungen des Verantwortlichen in einer Form, die nachträgliche Änderungen ausschließt.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer sichert dem Verantwortlichen zu, die für die beauftragte Tätigkeit erforderlichen technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes ergriffen zu haben und einzuhalten. Insbesondere wird zugesichert, dass der Auftragnehmer ein 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 Verarbeitung derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Die beim Auftragnehmer hinsichtlich der beauftragten Tätigkeit relevanten technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO sind im Anhang 2 zu dieser Vereinbarung, passend zum ermittelten Risiko unter der Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse aufgeführt.

(3) Der Auftragnehmer stellt sicher, dass die eingeräumten Zugriffsrechte auf Systeme des Verantwortlichen nicht durch Unbefugte verwendet werden können sowie, dass Daten des Verantwortlichen nicht durch Unbefugte eingesehen werden können.

(4) Der Auftragnehmer verpflichtet sich zu einer ausreichenden Datensicherung, soweit Daten des Verantwortlichen beim Auftragnehmer gespeichert werden. Insbesondere sichert der Auftragnehmer ausreichende Vorkehrungen gegen Datenverlust, Nichtverfügbarkeit und Verbreitung von Malware zu.

(5) Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt: Zunächst wird der Schutzbedarf der personenbezogenen Daten, die verarbeitet werden, ermittelt (normal, hoch, sehr hoch). Die technischen und organisatorischen Maßnahmen werden anschließend unter Berücksichtigung des Risikos, das mit der Datenverarbeitung für die Rechte und Freiheiten der betroffenen Personen verbunden ist, ausgewählt. Das Risiko bestimmt sich nach der Schwere des möglichen physischen, materiellen oder immateriellen Schadens für die betroffene Person (vernachlässigbar, begrenzt, wesentlich, maximal) sowie der Wahrscheinlichkeit, dass ein solcher Schaden eintritt (vernachlässigbar, begrenzt, wesentlich, maximal).

(6) 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 in dokumentierter Form abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

(7) Soweit der Auftragnehmer für den Verantwortlichen Wartungsarbeiten an IT-Systemen durchführt, gelten zusätzlich die folgenden Vereinbarungen:

(7.1) Der Auftragnehmer darf im Rahmen der Wartung nur auf personenbezogene Daten des Verantwortlichen zugreifen, wenn dies für die Durchführung der Wartung erforderlich ist. Dem Auftragnehmer ist es bei der Wartung untersagt, personenbezogene Daten des Verantwortlichen auf eigenen Systemen oder Datenträgern zu speichern, es sei denn der Verantwortliche weist ihn hierzu an.

(7.2) Fernwartungsarbeiten hat der Auftragnehmer dem Verantwortlichen im Vorfeld anzukündigen. Der Verantwortliche ist berechtigt, die Durchführung der Fernwartung mit zu verfolgen. Auf Anfrage und soweit erforderlich, wirkt der Auftragnehmer an der Konfiguration technischer Kontrolleinrichtungen mit.

(7.3) Die direkte Fernwartung ist nur vom Server-Standort des Auftragnehmers (Am Springborn 1, 51063 Köln) aus zulässig. Datenübertragungen zu Zwecken der Fernwartung müssen in verschlüsselter Form, die dem Stand der Technik entspricht, erfolgen. Der Auftragnehmer verwendet nach dem Stand der Technik hinreichend sichere Authentisierungsverfahren.

§ 6 Datengeheimnis, Vertraulichkeit der Daten

(1) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen sowie Datensicherheitsmaßnahmen des Verantwortlichen vertraulich zu behandeln. Diese Verpflichtung besteht auch nach Beendigung dieses Vertrages fort.

(2) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor der Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und diese sich schriftlich zur Verschwiegenheit und Vertraulichkeit – auch nach der Beendigung ihres Beschäftigungsverhältnisses – verpflichtet zu haben. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften. Die Vertraulichkeitspflichten gelten auch nach Beendigung dieser Vereinbarung fort. Des Weiteren sichert der Auftragnehmer zu, seine Mitarbeiter auf die Folgen der Verletzung von Privat-, Betriebs- und Geschäftsgeheimnissen hinzuweisen.

(3) Der Auftragnehmer verwendet die zur automatisierten Datenverarbeitung überlassenen bzw. zur Verfügung gestellten personenbezogenen Daten, Schriftstücke und Datenbestände für keine anderen, insbesondere keine eigenen Zwecke. Datenträger, die vom Verantwortlichen stammen bzw. für diesen genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert. Ferner wird der Auftragnehmer die Daten des Verantwortlichen strikt von sonstigen Datenbeständen trennen.

(4) Kopien oder Duplikate von personenbezogenen Daten (unabhängig in welcher Form diese vorliegen) werden nicht ohne Wissen und Genehmigung des Verantwortlichen erstellt. Unberührt bleibt die Herstellung von Backups, wenn die Anfertigung dieser erforderlich ist, um ordnungsgemäß die Daten zu verarbeiten oder um gesetzliche Aufbewahrungspflichten zu erfüllen.

(5) Die bei der Durchführung der Tätigkeiten für den Verantwortlichen vom Auftragsverarbeiter sowie etwaigen weiteren Auftragsverarbeitern eingesetzten Personen werden im datenschutzrechtlichen Sinne als Personen, die an der Tätigkeit von Rechtsanwälten, Steuerberatern und Wirtschaftsprüfern mitwirken, i.S.d. § 203 StGB angesehen. Der Auftragsverarbeiter sowie etwaige weitere Auftragsverarbeiter setzen nur solche Personen zur Auftragserfüllung ein, die auf besondere Geheimhaltungspflichten wie das Berufsgeheimnis von Rechtsanwälten gemäß § 2 Abs. 5 Berufsordnung für Rechtsanwälte (BORA) i.V.m. § 43a Abs. 2 Bundesrechtsanwaltsordnung (BRAO), das Berufsgeheimnis von Steuerberatern gemäß § 57 Abs. 1 i.V.m. § 62 Steuerberatungsgesetz (StBerG) sowie das Berufsgeheimnis von Wirtschaftsprüfern gemäß § 43 Abs. 1 S. 1 i.V.m. § 50 Berufsordnung der Wirtschaftsprüfer (WiPrO) verpflichtet wurden (Anhang 1 - weitere Auftragnehmer) und für die keine Unverträglichkeit mit der Verpflichtung als Gehilfe besteht (z.B. aufgrund des Vorliegens einer einschlägigen Straftat). Der Auftragsverarbeiter sowie etwaige weitere Auftragsverarbeiter sichern zu, die von ihnen eingesetzten Personen auf die Folgen der Verletzung der besonderen Geheimhaltungspflichten nach § 203 StGB hinzuweisen.

§ 7 Unterstützung des Verantwortlichen

(1) Auskünfte an Dritte oder an Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den oder aufgrund bestehender Vereinbarung mit dem Verantwortlichen erteilen. Gleiches gilt für die Herausgabe von Schriftstücken oder Datensätzen.

(2) Der Auftragnehmer hat auf Anfragen des Verantwortlichen unverzüglich zu reagieren, damit die gesetzlichen Fristen bei Informations- und Auskunftspflichten seitens des Verantwortlichen eingehalten werden können.

(3) Soweit ein Betroffener seine Rechte nach der DSGVO, insbesondere nach Kapitel III oder anderer datenschutzrechtlicher Bestimmungen unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten und diesen bei der Bearbeitung dieser Rechte wenn nötig zu unterstützen. Er unterlässt es, eigenverantwortlich Auskünfte zu erteilen, es sei denn, der Verantwortliche hat ihn zuvor dazu aufgefordert.

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

(5) Der Auftragnehmer benennt einen Ansprechpartner, der den Verantwortlichen bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Verarbeitung im Auftrag entstehen, unterstützt und teilt dem Verantwortlichen dessen Kontaktdaten unverzüglich mit.

(6) Der Auftragnehmer unterstützt den Verantwortlichen bei einer anstehenden Datenschutz-Folgenabschätzung sowie der Führung des Verzeichnisses von Verarbeitungstätigkeiten im notwendigen Umfang, sofern dies personenbezogene Daten des Verantwortlichen betrifft. Die hierzu notwendigen Angaben stellt er dem Verantwortlichen zur Verfügung.

(7) Der Auftragnehmer hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten des Verantwortlichen mitzuwirken. Er hat dem Verantwortlichen die erforderlichen Angaben und Dokumente auf Anfrage offen zu legen.

(8) Der Auftragnehmer führt selbst ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung und beachtet hierbei die Vorgaben des Art. 30 Abs. 2 DSGVO.

§ 8 weitere Auftragnehmer

(1) Die Beauftragung von weiteren Auftragnehmern zur Verarbeitung von Daten des Verantwortlichen ist dem Auftragnehmer nur mit Genehmigung des Verantwortlichen gestattet, Art. 28 Abs. 2 DSGVO, welche in Textform zu erfolgen hat.

(2) Die Zustimmung kann nur dann erteilt werden, wenn der Auftragnehmer dem Verantwortlichen Namen und Anschrift sowie die vorgesehene Tätigkeit des weiteren Auftragnehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den weiteren Auftragnehmer unter Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die Dokumentation dazu ist dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.

(3) Eine Beauftragung weiterer Auftragnehmer durch den Auftragnehmer in Drittstaaten darf nur dann erfolgen, wenn die besonderen Voraussetzungen des Art 44 ff. DSGVO erfüllt sind (bspw. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

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

(5) Der Vertrag mit dem weiteren Auftragnehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

(6) Die Weiterleitung von Daten an den weiteren Auftragnehmer ist erst zulässig, wenn dieser die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat und der Auftragnehmer die Einhaltung dieser Pflichten durch den weiteren Auftragnehmer regelmäßig überprüft.

(7) Der Auftragnehmer haftet gegenüber dem Verantwortlichen dafür, dass der weitere Auftragnehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

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

(9) Nicht als weitere Auftragnehmer im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen i.d.R. z.B. Telekommunikationsleistungen oder Reinigungskräfte. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(10) Die vom Auftragnehmer bereits eingesetzten weiteren Auftragnehmer sind im Anhang 1 zu diesem Vertrag aufgeführt. Mit dem Einsatz dieser weiteren Auftragnehmer erklärt sich der Verantwortliche einverstanden.

(11) Der Auftragnehmer hat die Einhaltung der Pflichten des jeweiligen weiteren Auftragnehmers zu überprüfen. Das Ergebnis der Überprüfung ist zu dokumentieren und dem Verantwortlichen auf Verlangen zugänglich zu machen.

§ 9 Aufsichtsbehörden und Verstöße gegen Vorgaben

(1) Der Auftragnehmer ist verpflichtet, dem Verantwortlichen Kontrollen oder Ermittlungen durch Aufsichtsbehörden oder durch Revisoren/Prüfer unverzüglich mitzuteilen, sofern dies personenbezogene Daten des Auftraggebers betrifft.

(2) Der Auftragnehmer unterrichtet den Verantwortlichen unverzüglich bei Störungen des Betriebsablaufs, bei Eintritt von oder Verdacht auf Verletzung datenschutzrechtlicher Vorschriften bzw. den in dieser Vereinbarung getroffenen Festlegungen sowie bei anderen Fehlern bzw. Unregelmäßigkeiten im Rahmen der Auftragsarbeiten für den Verantwortlichen. Gleiches gilt, wenn der Auftragnehmer feststellt, dass die bei ihm getroffenen technischen und organisatorischen Maßnahmen den gesetzlichen Anforderungen nicht genügen.

(3) Die entsprechende Meldung des Auftragnehmers hat die Vorgaben aus Art. 33 Abs. 3 DSGVO zu berücksichtigen; er sichert ferner zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 oder 34 DSGVO angemessen zu unterstützen

(4) Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragnehmer nur nach vorheriger schriftlicher Weisung durchführen. Der Auftragnehmer wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen 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 nach Überprüfung bestätigt oder geändert wird.

(5) Bei Konsultationen der Aufsichtsbehörde wird der Verantwortliche seitens des Auftragnehmers unterstützt.

§ 10 Löschung und Rückgabe von Daten

(1) Eine Berichtigung, Löschung oder Sperrung von Daten erfolgt ausschließlich im Rahmen der schriftlichen Weisung des Verantwortlichen.

(2) Test- und Ausschussmaterial ist durch den Auftragnehmer unverzüglich unter Einhaltung mindestens der Sicherheitsstufe P-4 der DIN 66399 (hinsichtlich etwaiger Schriftstücke) bzw. mindestens gemäß der Sicherheitsstufe H-4 bzw. T-4 der DIN 66399 (hinsichtlich magnetischer Datenträger) zu vernichten. Die Vernichtung der Daten wird nach Aufforderung des Verantwortlichen vom Auftragnehmer durch Zusendung eines geeigneten Nachweises bestätigt.

(3) Sofern Daten(-sätze) des Verantwortlichen auf Systemen des Auftragnehmers gespeichert wurden, sind diese Daten(-sätze) nach Abschluss der jeweiligen Auftragstätigkeiten dem Verantwortlichen in einer migrationsfähigen Form auszuhändigen bzw. nach Weisung des Verantwortlichen unverzüglich zu löschen. Das Löschen der Daten(-sätze) hat so zu erfolgen, dass eine Rekonstruktion der Datensätze ausgeschlossen werden kann oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Auf Anfrage des Verantwortlichen hat der Auftragnehmer die Logdatei über den Löschvorgang vorzulegen. Der Verantwortliche bestätigt in Textform die Rückgabe der Daten in einem migrationsfähigen Format.

(4) Nach Abschluss der jeweiligen Auftragsarbeiten hat der Auftragnehmer dem Verantwortlichen sämtliche in seinen Besitz gelangten Unterlagen und Datensätze, die im unmittelbaren Zusammenhang mit dem Auftragsverhältnis stehen, auszuhändigen bzw. weisungsgemäß zu löschen und dies im Falle der Löschung unter Angabe des Löschdatums schriftlich zu bestätigen.

(5) Dem Auftragnehmer ist es untersagt, im Rahmen der Auftragsarbeiten verarbeitete personenbezogene Daten länger zu speichern, als dies mit dem Verantwortlichen schriftlich vereinbart ist.

(6) Unterliegen vom Auftragnehmer zu Zwecken der Dokumentation der Auftragstätigkeiten angefertigte Unterlagen gesetzlichen Aufbewahrungspflichten, sind diese durch den Auftragnehmer bis zum Ablauf der geforderten Frist datenschutzrechtlich zu sperren.

§ 11 Kontrollpflichten

(1) Der Auftragnehmer erklärt sich damit einverstanden, dass der Verantwortliche bzw. ein von ihm beauftragter Dritter während der üblichen Betriebs- und Geschäftszeiten und ohne Störung des Betriebsablaufs berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz, die Datensicherheit bzw. der vertraglichen Vereinbarungen sowie die Angemessenheit der zugesicherten technischen und organisatorischen Maßnahmen in den Geschäftsräumen des Auftragnehmers 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).

(2) Der Auftragnehmer sichert zu, dass er bei Erforderlichkeit bei diesen Kontrollen unterstützend mitwirkt.

(3) Der Auftragnehmer verpflichtet sich, auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, Nachweise zu erbringen und Einsichtnahmen zu gewähren, die zur Durchführung einer Auftragskontrolle, bei der die Wirksamkeit technischer und organisatorischer Maßnahmen überprüft wird, erforderlich sind.

§ 12 Beginn und Ende des Vertrages

(1) Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages und beginnt somit zum 08.11.2019.

(2) Der Verantwortliche kann das Auftragsverhältnis jederzeit ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer in schwerwiegender Weise gegen die Bestimmungen dieses Vertrages oder gegen gesetzliche Bestimmungen verstößt, der Auftragnehmer eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schwerwiegenden Verstoß dar.

§ 13 Schlussbestimmungen

(1) Sofern eine Vertragspartei besonderen oben nicht genannten Geheimnisschutzregeln unterliegt und sie dies der anderen Partei zu Vertragsbeginn schriftlich mitteilt, ist auch diese Partei verpflichtet, die Geheimnisschutzregelungen zu beachten.

(2) Sollte das Eigentum des Verantwortlichen beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf die Datenträger und die Datenbestände des Verantwortlichen ausgeschlossen.

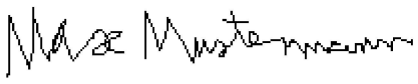
(3) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der für den Verantwortlichen verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Sollten einzelne Teile des Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

(5) Ergänzungen oder Änderungen zu diesem Vertrag unterliegen der Schriftform.

Musterort, 25.05.2020 — Köln,

Ort, Datum — Ort, Datum



Unterschrift Verantwortlicher

Auflistung der beauftragten Dienstleistungen

Dienstleistung(en)	Bereitstellung einer Software zur Erfassung von Arbeits- und Projektzeiten als On-Premises-Version sowie die Übermittlung der in der Software erfassten Daten an den Auftragnehmer zwecks Erbringung von Support-Dienstleistungen (Beantwortung von Fragen, Fehleranalyse)
Art der personenbezogenen Daten	Personalstammdaten (Name, Vorname, Geburtsdatum, Abteilung, Erfassungsstart, Urlaubsanspruch, Telefonnummer, Windows-Anmeldename) Arbeitszeiten, Projektzeiten, Urlaubstage, Krankheitstage, Termine Projektstammdaten (Kunde/Auftrag/Arbeitsschritt)
Kategorien betroffener Personen	Freie Mitarbeiter, Lohnempfänger, Gehaltsempfänger, Kunden (bei Projektzeiterfassung)
Art und Zweck der Verarbeitung der Daten	Erfassung der täglichen Arbeitszeit zum Führen eines Arbeits- und Projektzeitkontos. Monatliche Erstellung eines Stundenzettels pro Mitarbeiter als Basis für Lohn- & Gehaltsabrechnung sowie die Auswertung geleisteter Arbeitszeiten für Kunden, Aufträge und Arbeitsschritte der Mitarbeiter

Auflistung der beauftragten weiteren Auftragnehmer einschließlich der Verarbeitungsstandorte

Weitere Auftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	Surfplanet GmbH, Köln
Verarbeitungsstandort (wenn abweichend)	Am Springborn 1 51063 Köln
Art der Dienstleistung	Betrieb des Rechenzentrums (Server-Housing)

Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG

Zutrittskontrolle zum Server (Am Springborn 1, 51063 Köln)

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ► Alarmanlage
- ► Automatisches Zugangskontrollsystem
- ► Manuelles Schließsystem (zum Öffnen des Serverschranks)
- ► Biometrische Zugangssperren
- ► Videoüberwachung der Zugänge
- ► Bewegungsmelder
- ► Sicherheitsschlösser
- ► Schlüsselregelung
- ► Personenkontrolle beim Empfang
- ► Protokollierung der Besucher

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ► Einsatz von gesicherten KVM-Lösungen zur Steuerung der Server
- ► Zuordnung von Benutzerrechten
- ► Erstellen von Benutzerprofilen
- ► Passwortvergabe
- ► Authentifikation mit biometrischen Verfahren
- ► Authentifikation mit Benutzername / Passwort
- ► Zuordnung von Benutzerprofilen zu IT-Systemen
- ► Einsatz von VPN-Technologie
- ► Schlüsselregelung (Schlüsselausgabe etc.)
- ► Protokollierung der Besucher
- ► Einsatz von Anti-Viren-Software
- ► Verschlüsselung von Datenträgern in Laptops / Notebooks
- ► Einsatz einer Software-Firewall

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ► Erstellen eines Berechtigungskonzepts
- ► Verwaltung der Rechte durch Systemadministrator
- ► Anzahl der Administratoren auf das Notwendigste reduziert
- ► Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ► Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ► Sichere Aufbewahrung von Datenträgern
- ► Physische Löschung von Datenträgern vor Wiederverwendung
- ► Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- ► Protokollierung der Vernichtung
- ► Verschlüsselung von Datenträgern

Weitergabekontrolle

Maßnahmen, die gewährleisten, 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ► Einrichtungen von VPN-Tunneln
- ► Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ► E-Mail-Verschlüsselung
- ► Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ► Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ► Protokollierung der Eingabe, Änderung und Löschung von Daten
- ► Übersicht mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
- ► Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- ► Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ► Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ► Vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ► Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
- ► Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- ► Auftragnehmer hat Datenschutzbeauftragten bestellt
- ► Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ► Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ► Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- ► Vertragsstrafen bei Verstößen

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ► Unterbrechungsfreie Stromversorgung (USV)
- ► Klimaanlage in Serverräumen
- ► Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ► Schutzsteckdosenleisten in Serverräumen
- ► Feuer- und Rauchmeldeanlagen
- ► Feuerlöschgeräte in Serverräumen
- ► Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ► Erstellen eines Backup- & Recoverykonzepts
- ► Testen von Datenwiederherstellung
- ► Erstellen eines Notfallplans
- ► Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Trennungsgebot

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

- ► Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ► Logische Mandantentrennung (softwareseitig)
- ► Erstellung eines Berechtigungskonzepts
- ► Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ► Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ► Pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Speicherung auf einem getrennten IT-System
- ► Festlegung von Datenbankrechten
- ► Trennung von Produktiv- und Testsystem

Allgemeines zum Bürobetrieb

Alle Mitarbeiter der TempoBill GmbH arbeiten an digitalen Arbeitsplätzen. Dies sind windowsbasierte Hardware-Terminals, die über keine Möglichkeit der lokalen Speicherung von Daten verfügen.

- ► die Arbeit erfolgt ausschließlich in Terminal-Sitzungen, die auf einem unserer Server im Rechenzentrum in Köln
- ► die Anmeldung an den Terminal-Sitzungen erfolgt im 2-Faktor-Verfahren biometrisch und via NFC-Buchungsausweis
- ► der gesamte Traffic (Surfen im Web, E-Mail-Abfrage, Fernwartungen etc.) erfolgt innerhalb der Terminal-Sitzung
- ► der Zugang zu den Terminal-Sitzungen ist nur von bestimmten IP-Adressen aus erlaubt (Büro, HomeOffice)

Anonymisierung von Daten

Es lässt sich ein Bericht mit Informationen erzeugen, welche personenbezogenen Daten wo aktuell in der Datenbank gespeichert sind.

Bei der Erstellung und Übermittlung von Datensicherungen an Auftragnehmer werden persönliche Merkmale anonymisiert, die auf die Identität des Mitarbeiters hinweisen. Dabei handelt es sich um Vorname, Nachname, Geburtsdatum sowie den Windows-Anmeldenamen. Der Speicherort der verschlüsselten Zuordnungsdatei kann frei gewählt werden.

Das Entfernen eine Mitarbeiters erfolgt über die Zuordnungsdatei. Bei einer Löschung eines Mitarbeiter aus dieser Datei werden automatisch die in der Anwendungsdatenbank gespeicherten Informationen anonymisiert, wodurch sowohl der Löschpflicht als auch der gesetzlichen Aufbewahrungspflicht Rechnung getragen wird.

Bezüglich der Löschung wird ein Bericht erzeugt, der Informationen darüber enthält, wie viele Datensätze des Mitarbeiters in welchen Datenbanktabellen (Zeitbuchungen, Projektbuchungen, Urlaub, Krankheit) anonymisiert wurden.