ALLGEMEINE GESCHÄFTSBEDINGUNGEN DER TROI GMBH FÜR DIE ERBRINGUNG VON SAAS-LEISTUNGEN

VERSION: AGB-SAAS-2026-10

TEIL 1: GEGENSTAND DIESER AGB, LEISTUNG UND VERGÜTUNG

1. Gegenstand dieser AGB und Vertragsschluss

1.1 Diese AGB gelten für sämtliche Leistungen der TROI GmbH (kurz: „TROI“). Der Vertrag kann durch elektronischen Bestellprozess, durch individuelle Vereinbarung oder durch Annahme eines Angebots zustande kommen.

Im Falle eines elektronischen Bestellprozesses stellen die im Online-Bestellprozess enthaltenen Angaben noch kein verbindliches Angebot von TROI dar. Vielmehr gibt der Kunde mit Abschluss des elektronischen Bestellprozesses ein verbindliches Angebot zum Abschluss eines Vertrags über die im Warenkorb oder im Rahmen des Bestellprozesses ausgewählten Leistungen, einschließlich der dabei einbezogenen Vertragsunterlagen, insbesondere Leistungsbeschreibungen, Auftragsverarbeitungsvereinbarungen, Systemvoraussetzungen und dieser AGB, ab. Der Vertrag kommt erst durch ausdrückliche Annahmeerklärung von TROI oder durch Freischaltung der gebuchten Leistungen zustande.

Der Vertrag einschließlich seiner Anlagen samt dieser AGB wird im Folgenden gemeinsam auch als „Vertrag“ bezeichnet.

Die im Rahmen des elektronischen Bestellprozesses einbezogenen Vertragsunterlagen können vom Kunden vor Abschluss des Bestellprozesses gespeichert oder ausgedruckt werden.

1.2 Die Leistungen von TROI richten sich ausschließlich an Unternehmer im Sinne des § 14 BGB und nicht an Verbraucher. Der Kunde sichert zu, bei Abschluss des Vertrags in Ausübung seiner gewerblichen oder selbständigen beruflichen Tätigkeit zu handeln. Die den Vertrag für den Kunden abschließende Person sichert zudem zu, zum Abschluss des Vertrags im Namen des Kunden berechtigt zu sein.

1.3 Im Falle von Widersprüchen gilt für die Vertragsunterlagen folgende Rangfolge: a) individuelle Vereinbarungen und Angebote von TROI in Textform, b) Angaben im elektronischen Bestellprozess, c) Leistungsbeschreibungen, d) Systemvoraussetzungen und technische Dokumentationen, e) diese AGB.

Für datenschutzrechtliche Regelungen gehen die Bestimmungen einer Auftragsverarbeitungsvereinbarung den übrigen Vertragsunterlagen im Falle von Widersprüchen vor.

AGB des Kunden gelten nicht, auch dann nicht, wenn ihnen TROI nicht ausdrücklich widersprochen hat.

1.4 Der Vertrag einschließlich der im Angebot oder im elektronischen Bestellprozess einbezogenen Anlagen enthält zusammen mit diesen AGB abschließend alle Regelungen und Vereinbarungen der Parteien zum Vertragsgegenstand. Frühere Angebote, Präsentationen, Projektbeschreibungen oder sonstige vorvertragliche Erklärungen werden nicht Vertragsbestandteil. Nebenabreden sind nicht getroffen.

Andere oder weitere Leistungen, als im Vertrag und der Leistungsbeschreibung beschrieben, schuldet TROI nicht.

1.5 Vertragsgegenstand kann bei gesonderter Einzelbeauftragung ferner die Erbringung von weiteren Leistungen sein. Soweit dafür keine gesonderten Allgemeinen Geschäftsbedingungen von TROI gelten, enthalten die hiesigen AGB die Rahmenbedingungen für diese weiteren Leistungen und gelten deren Regelungen entsprechend.

2. Leistungen von TROI

2.1 TROI schuldet ausschließlich die im Vertrag, insbesondere der Anlage zur Leistungsbeschreibung, im Einzelnen genannten Leistungen.

2.2 TROI erbringt die Leistungen als technische und organisatorische SaaS- und Unterstützungsleistungen. TROI schuldet keine rechtliche, steuerliche, buchhalterische, arbeitsrechtliche oder betriebswirtschaftliche Prüfung, Beratung oder Bewertung des Kunden, seiner Daten, Prozesse, Einstellungen, Auswertungen oder Arbeitsergebnisse, soweit dies nicht ausdrücklich vereinbart ist.

3. Vergütung, Abrechnung, Preisanpassung

3.1 Der Kunde schuldet die im Vertrag, insbesondere im Angebot oder im elektronischen Bestellprozess, genannte Vergütung.

3.2 Die Vergütung kann wiederkehrende Gebühren, Einmalgebühren sowie nutzungs- oder verbrauchsabhängige Entgelte enthalten.

Nutzungs- oder verbrauchsabhängige Entgelte („Verbrauchseinheiten“) können insbesondere auf Grundlage der im Vertrag oder in der Leistungsbeschreibung festgelegten Nutzungseinheiten, etwa ausgeführter Workflows oder vergleichbarer Nutzungsparameter, berechnet werden.

Beginnt die Vertragslaufzeit während eines laufenden Kalendermonats, ist die monatliche Vergütung zeitanteilig für die verbleibenden Kalendertage geschuldet.

3.3 Alle im Vertrag genannten Preise sind Nettopreise und verstehen sich zzgl. der gesetzlichen Umsatzsteuer.

3.4 Gerät der Kunde mit mindestens einer wiederkehrenden Gebühr mit mehr als 14 Tagen in Zahlungsverzug, ist TROI berechtigt, die SaaS- und Hosting-Leistungen vorübergehend ganz oder teilweise zu sperren; diese Sperrung ist dem Kunden mindestens 7 Kalendertage zuvor anzukündigen. Der Kunde bleibt während der Dauer der Sperrung verpflichtet, die vereinbarte Vergütung zu zahlen. TROI wird die Leistungen wieder freischalten, sobald sämtliche fälligen Forderungen, wegen derer die Sperrung erfolgt ist, vollständig an TROI bezahlt sind.

3.5 TROI darf mit einer Ankündigungsfrist von 3 Monaten zum Zeitpunkt der nächsten Vertragsverlängerung zum Ausgleich von Personal- und sonstigen Kostensteigerungen die Monats- oder Jahresgebühren ganz oder teilweise im angemessenen Umfang erhöhen, maximal jedoch um bis zu 20 %. Dies hat TROI vorab dem Kunden in Textform mitzuteilen. Dem Kunden steht es frei, sein ordentliches Kündigungsrecht auszuüben.

3.6 Soweit der Kunde Leistungen bei TROI beauftragt, die über die im Vertrag genannten Leistungen hinausgehen, gelten die im Vertrag genannten Preise entsprechend, soweit nicht vorrangig anderweitige Absprachen getroffen sind.

3.7 TROI wird dem Kunden die vereinbarten Leistungen gemäß dem vereinbarten Abrechnungszyklus in elektronischer Form in Rechnung stellen.

3.8 Der Kunde gerät mit Ablauf eines vereinbarten Zahlungsziels oder, soweit ein solches nicht vereinbart ist, spätestens 14 Tage nach Fälligkeit und Zugang der Rechnung ohne weitere Mahnung in Verzug. Während des Verzugs ist TROI berechtigt, die gesetzlichen Verzugszinsen zu verlangen. TROI ist zudem berechtigt, im Falle des Zahlungsverzugs die gesetzliche Verzugskostenpauschale gemäß § 288 Abs. 5 BGB zu verlangen.

3.9 Überschreitet die tatsächliche Nutzung der Verbrauchseinheiten, insbesondere der Business-Actions, das für den jeweiligen Abrechnungszeitraum vertraglich vereinbarte oder in der gebuchten Lizenzklasse enthaltene Nutzungsvolumen, wird die darüber hinausgehende Nutzung nach den dafür vereinbarten Konditionen, anderenfalls nach der gültigen Preisliste, zusätzlich berechnet.

4. Vertragslaufzeit und Kündigung

4.1 Die Vertragslaufzeit beträgt initial 36 Monate, soweit nicht ausdrücklich eine andere Laufzeit vereinbart ist. Die Vertragslaufzeit beginnt mit dem Tag des Vertragsschlusses, soweit im Vertrag nicht ausdrücklich ein anderer Beginn geregelt ist.

Die Vertragslaufzeit verlängert sich jeweils automatisch um weitere 12 Monate, sofern sie nicht von einer Partei mit einer Frist von drei Monaten zum jeweiligen Laufzeitende gekündigt wird.

Im Übrigen ist das Recht zur ordentlichen Kündigung ausgeschlossen.

4.2 Dem Kunden steht frei, im Rahmen der ordentlichen Kündigung nach Ziffer 4.1 zum Laufzeitende alle oder auch nur einzelne zu diesem Zeitpunkt vertragsgegenständlichen Nutzerlizenzen, nutzungsabhängige Kontingente oder Nutzungspakete, Module oder Zusatzfunktionen zu kündigen, was er in seiner Kündigungserklärung anzugeben hat. Gibt der Kunde dazu nichts an, bezieht sich im Falle einer Kündigung diese auf alle zum Zeitpunkt des Laufzeitendes vertragsgegenständlichen Nutzerlizenzen, nutzungsabhängige Kontingente oder Nutzungspakete, Module und Zusatzfunktionen.

4.3 Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt beiden Parteien vorbehalten. Für TROI liegt ein solcher insbesondere vor, wenn der Kunde für zwei aufeinanderfolgende Monate mit der Entrichtung eines nicht unerheblichen Teils der geschuldeten Vergütung in Verzug gerät oder der Kunde rechtswidrige Inhalte oder Daten speichert, verarbeitet oder bereitstellt oder gegen geltendes Recht verstößt.

4.4 Eine Kündigung durch den Kunden gem. § 543 II Nr. 1 BGB wegen Nichtgewährung des vertragsgemäßen Gebrauchs ist erst zulässig, wenn er TROI ausreichende Gelegenheit zur Mängelbeseitigung gegeben hat und diese fehlgeschlagen ist.

4.5 Kündigungen bedürfen mindestens der Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist. Soweit von TROI bereitgestellt, kann die Kündigung alternativ auch über ein Portal erfolgen.

TEIL 2: SOFTWARE AS A SERVICE (SAAS) UND HOSTING

5. Bereitstellung der SaaS-Leistungen

5.1 TROI stellt dem Kunden über das Internet im Rahmen der in Ziffer 10 dieser AGB definierten Verfügbarkeiten die Nutzung der im Vertrag genannten Softwarefunktionalitäten zur Verfügung (kurz: „Software“). Die Software verbleibt dabei auf dem Server von TROI, der Kunde nutzt deren Funktionen über das Internet („Software as a Service“, kurz: „SaaS“). TROI schuldet keine Überlassung der Software, Vertragsgegenstand ist vielmehr ausschließlich die Einräumung des vorgenannten Zugangs über das Internet. Neben dem Kunden nutzen auch andere Kunden diese Software.

5.2 Anbindungsmöglichkeit von Kunden-KI:

Soweit die Software Schnittstellen oder sonstige technische Funktionen zur Anbindung von KI-Systemen, Large Language Models (LLM) oder vergleichbaren Diensten des Kunden oder von diesem beauftragter Dritter an die Software oder zur Nutzung der Software durch solche Systeme ermöglicht, schuldet TROI ausschließlich die vertragsgemäße technische Funktionalität der von TROI hierfür bereitgestellten Schnittstellen und Funktionen.

Die Auswahl, Bereitstellung, Konfiguration und Nutzung des angebundenen KI-Systems oder Dienstes obliegt dem Kunden. TROI schuldet insbesondere nicht die Verfügbarkeit, Funktionsfähigkeit oder Ergebnisse des angebundenen KI-Systems oder Dienstes und – soweit dieses von einem Dritten bereitgestellt wird – auch nicht die hierfür erforderlichen Nutzungsrechte, Nutzungskontingente oder sonstigen Leistungen dieses Dritten.

Von TROI bereitgestellte KI-Funktionalitäten:

Soweit TROI dagegen gemäß dem Vertrag oder der Leistungsbeschreibung selbst KI-basierte Funktionen als Bestandteil der Software bereitstellt, können deren Ergebnisse auf automatisierten Analysen und probabilistischen Modellen beruhen und im Einzelfall unvollständig, fehlerhaft oder nicht eindeutig sein. Der Kunde bleibt verpflichtet, solche Ergebnisse vor deren Verwendung eigenverantwortlich zu prüfen. Von TROI bereitgestellte KI-basierte Funktionen dienen, soweit im Vertrag oder der Leistungsbeschreibung nicht ausdrücklich etwas anderes bestimmt ist, der Unterstützung des Kunden bei der Nutzung der Software sowie der Auswertung, Strukturierung oder Vorbereitung von Informationen. Sie ersetzen keine eigenverantwortliche fachliche, rechtliche, steuerliche, buchhalterische oder betriebswirtschaftliche Prüfung, Bewertung oder Entscheidung durch den Kunden. Der Kunde bleibt für die Bewertung, Auswahl, Freigabe und Verwendung der Ergebnisse sowie für sämtliche darauf beruhenden Entscheidungen verantwortlich.

5.3 TROI ist berechtigt, die Software während der Vertragslaufzeit fortlaufend weiterzuentwickeln, anzupassen oder zu aktualisieren, insbesondere durch Fehlerbehebungen sowie sonstige technische oder funktionale Änderungen.

Der Kunde erhält im Rahmen der SaaS-Leistungen Zugriff auf die jeweils von TROI aktuell bereitgestellte Version der Software; ein Anspruch auf die Nutzung einer bestimmten Version oder eines bestimmten Funktionsstands besteht nicht.

Weiterentwicklungen, Anpassungen und Aktualisierungen der Software werden von TROI zentral bereitgestellt. Ein Ausschluss oder Aufschub einzelner Änderungen oder Aktualisierungen durch den Kunden ist nicht möglich.

Soweit TROI gemäß dem Vertrag oder der Leistungsbeschreibung selbst KI-basierte Funktionen als Bestandteil der Software bereitstellt, gelten die vorstehenden Regelungen auch für diese Funktionen. TROI ist insbesondere berechtigt, solche KI-basierten Funktionen weiterzuentwickeln, anzupassen, zu ersetzen oder einzuschränken, soweit dies aufgrund technischer, rechtlicher, regulatorischer oder sicherheitsbezogener Anforderungen, zur Vermeidung von Missbrauch, zur Wahrung der Rechte Dritter oder aufgrund von Änderungen eingesetzter Drittanbieter-Services erforderlich oder sachlich gerechtfertigt ist.

Voraussetzung ist, dass die Änderungen für den Kunden zumutbar sind und nicht zu einer wesentlichen Einschränkung des vertragsgemäßen Funktionsumfangs führen oder aus Gründen des technologischen Fortschritts, der IT-Sicherheit oder aufgrund gesetzlicher beziehungsweise regulatorischer Anforderungen erforderlich sind.

Über wesentliche Änderungen der Software informiert TROI den Kunden in geeigneter Weise, insbesondere über Release Notes oder Hinweise im Login-Bereich.

5.4 Der Kunde muss während der Vertragslaufzeit bei sich für das Vorhandensein der nötigen Systemvoraussetzungen sorgen, die in der Anlage Leistungsbeschreibung definiert sind.

5.5 Übergabepunkt der Leistung ist die Schnittstelle der von TROI betriebenen Serversysteme zum Internet. Von TROI daher nicht geschuldet ist insbesondere die Herstellung und Aufrechterhaltung der Datenverbindung zwischen den IT-Systemen des Kunden und dem Übergabepunkt von TROI.

5.6 Soweit die Software Schnittstellen, Integrationen oder Anbindungen an Systeme, Dienste, Plattformen oder Anwendungen Dritter enthält oder ermöglicht, schuldet TROI nicht die Verfügbarkeit, Funktionsfähigkeit oder unveränderte Fortführung dieser Drittangebote. Änderungen, Einschränkungen oder die Einstellung solcher Drittangebote können Auswirkungen auf die Funktionsfähigkeit der jeweiligen Schnittstellen, Integrationen oder Anbindungen haben.

5.7 TROI ist berechtigt, den Zugang zu Inhalten, Daten, Funktionen oder einzelnen Leistungen vorübergehend ganz oder teilweise zu sperren, falls ein hinreichender Verdacht besteht, dass über die Software rechtswidrige Inhalte verarbeitet, gespeichert oder bereitgestellt werden oder sonst gegen geltendes Recht verstoßen wird. Dies gilt insbesondere im Falle von Ermittlungen staatlicher Behörden oder behördlicher Anordnungen oder der Geltendmachung von Ansprüchen durch Dritte, wie etwa einer Abmahnung des vermeintlich Verletzten, es sei denn, die Abmahnung ist offensichtlich unbegründet.

Die Sperrung ist, sofern technisch möglich und zumutbar, auf die vermeintlich rechtsverletzenden Inhalte, Daten, Funktionen oder Leistungen zu beschränken.

Der Kunde ist über die Sperrung unter Angabe der Gründe unverzüglich zu benachrichtigen und aufzufordern, die beanstandeten Inhalte zu entfernen oder die Rechtmäßigkeit nachzuweisen. Die Sperrung ist aufzuheben, sobald der Verdacht entkräftet ist oder der rechtswidrige Zustand beseitigt wurde.

6. Inhalt der Hosting-Leistungen

6.1 TROI stellt dem Kunden im Rahmen der SaaS-Leistungen den nach Maßgabe des Vertrags, der gebuchten Nutzerlizenzen („Seats“), Lizenzklassen sowie etwaiger zusätzlicher Module oder Zusatzfunktionen vereinbarten Speicherplatz zur Verfügung, um Daten im Rahmen der Software zu speichern und auf diese zuzugreifen (Hosting).

6.2 TROI schuldet im Rahmen der Hosting-Leistungen nur die Bereitstellung von Speicherplatz zur Nutzung durch den Kunden, nicht jedoch den Import, die Eingabe, die Pflege, die Aktualisierung oder sonstige Verwaltung von Daten. Vielmehr hat der Kunde die Pflicht, seine Daten initial in die Software einzuspeichern, sofern dies nicht explizit Teil des Angebots oder durch Einzelauftrag von TROI übernommen ist.

6.3 Es obliegt dem Kunden, gespeicherte Daten und Inhalte zu pflegen, ebenso, dass die Daten und Inhalte richtig, vollständig und auf dem neuesten Stand sind, und keinerlei Rechte oder Rechtsvorschriften, gleich, welcher Art, verletzen. Für die Beachtung etwaiger handels- oder steuerrechtlicher Aufbewahrungspflichten ist alleine der Kunde verantwortlich. TROI treffen hinsichtlich der vom Kunden gespeicherten Daten und Inhalte keine Verwahrungs- oder Obhutspflichten.

6.4 Die von TROI durchgeführten Datensicherungsmaßnahmen ergeben sich aus der zum Vertrag gehörenden Auftragsverarbeitungsvereinbarung. Darüber hinausgehende Datensicherungs- oder Wiederherstellungsmaßnahmen sind von TROI nicht geschuldet.

6.5 Vom Kunden gelöschte Daten oder Inhalte sind grundsätzlich unwiederbringlich gelöscht. Soweit TROI im Rahmen der geschuldeten Datensicherungsmaßnahmen noch eine Kopie vorhält, kann eine Wiederherstellung im Einzelfall gegen gesonderte Vergütung nach Aufwand erfolgen; ein Anspruch des Kunden auf Wiederherstellung besteht nicht.

7. Einräumung von Nutzungsrechten

7.1 Nutzungsumfang

Die Nutzung der Software erfolgt nutzerbezogen auf Basis der vom Kunden gebuchten Nutzerlizenzen („Full-Seats“, „Time-Seats“) und der diesen jeweils zugeordneten Lizenzklasse. Pro Nutzer ist jeweils eine eigene Nutzerlizenz erforderlich.

Nutzer sind die vom Kunden namentlich benannten und mit einem individuellen Zugang ausgestatteten Personen („Named User“), die berechtigt sind, die Software für den Kunden zu nutzen, unabhängig davon, ob die Software tatsächlich genutzt wird.

Nutzerlizenzen können unterschiedlichen Lizenzklassen zugeordnet sein, aus denen sich der jeweilige Funktionsumfang ergibt. Soweit der Vertrag für eine Lizenzklasse zusätzliche Nutzerlizenzen vorsieht, deren Funktionsumfang auf die Erfassung eigener Arbeits- und Projektzeiten beschränkt ist („Time-Seats“), dürfen die diesen Time-Seats zugeordneten Named User die Software ausschließlich in diesem Umfang nutzen.

Art und Anzahl der dem Kunden zustehenden Nutzerlizenzen einschließlich etwaiger Time-Seats sowie deren jeweiliger Funktionsumfang ergeben sich aus dem Vertrag und der Leistungsbeschreibung. Der Umfang der zulässigen Nutzung richtet sich darüber hinaus nach etwaigen zusätzlich vereinbarten Modulen oder Zusatzfunktionen.

Der Umfang der zulässigen Nutzung der Software ergibt sich aus dem Vertrag, der Anzahl und jeweiligen Lizenzklasse der gebuchten Nutzerlizenzen, etwaigen zusätzlich gebuchten Modulen oder Zusatzfunktionen sowie der Leistungsbeschreibung.

Eine gemeinsame Nutzung eines Nutzerkontos durch mehrere Personen ist nicht gestattet.

Der Kunde ist berechtigt, benannte Named User während der Vertragslaufzeit auszutauschen.

7.2 Nutzungsrechts-Einräumung/ Lizenzierung

Der Kunde darf die Software nur für eigene Zwecke und zur Bearbeitung von eigenen Daten und Inhalten nutzen.

Soweit dies zur Nutzung der Software über das Internet erforderlich ist, räumt TROI dem Kunden ein einfaches, nicht übertragbares und nicht unterlizenzierbares, auf die Vertragslaufzeit begrenztes Nutzungsrecht ein, die Software im vertraglich vereinbarten Umfang zu nutzen.

Der Kunde ist nicht berechtigt, die Software Dritten entgeltlich oder unentgeltlich zur Nutzung zur Verfügung zu stellen, die Software außerhalb der vertragsgegenständlichen Nutzung zu vervielfältigen, zu bearbeiten oder öffentlich zugänglich zu machen oder technische Schutzmaßnahmen oder Nutzungsbeschränkungen der Software zu umgehen. Eine Weitervermietung der Software wird dem Kunden somit ausdrücklich nicht gestattet.

7.3 Rechteinhaberschaft

Sämtliche Rechte an der Software sowie an den zugrunde liegenden Anwendungen, Datenbanken, Konzepten, technischen Lösungen, Dokumentationen, Inhalten, Kennzeichen, Marken und sonstigen Bestandteilen der SaaS-Leistungen stehen ausschließlich TROI beziehungsweise den jeweiligen Lizenzgebern zu. Soweit nicht ausdrücklich etwas anderes geregelt ist, werden dem Kunden keine weitergehenden Rechte an der Software oder den SaaS-Leistungen eingeräumt. Insbesondere erwirbt der Kunde keine Rechte am Quellcode, an Entwicklungsunterlagen, an technischen Konzepten oder an der zugrunde liegenden Softwarearchitektur.

Sämtliche Rechte an den im Rahmen der Erbringung der vertraglichen Leistungen durch TROI entwickelten Arbeitsergebnissen, wie etwa Software-Code, entstehen ausschließlich bei TROI. TROI räumt dem Kunden daran aber für die Laufzeit des Vertrages ein Nutzungsrecht ein, wie in Ziffer 7.2 bestimmt.

8. Nachträgliche Erweiterung von Nutzerlizenzen, Lizenzklassen, Modulen und Zusatzfunktionen

8.1 Während der Vertragslaufzeit können vom Kunden

- zusätzliche Nutzerlizenzen („Time-Seats“, „Full-Seats“) hinzugebucht,
- bestehende Nutzerlizenzen einer höheren Lizenzklasse zugeordnet,
- bestehende nutzungsabhängige Kontingente oder Nutzungspakete, insbesondere für Business-Actions, auf ein höheres Nutzungsvolumen erweitert, sowie
- zusätzliche Module oder Zusatzfunktionen gebucht

werden.

Solche zusätzlich gebuchten Nutzerlizenzen, höheren Lizenzklassen zugeordnete Nutzerlizenzen, erweiterten nutzungsabhängigen Kontingente oder Nutzungspakete sowie zusätzlich gebuchte Module oder Zusatzfunktionen werden Bestandteil des bestehenden Vertragsverhältnisses und unterfallen den hiesigen AGB. Für sie gilt insbesondere die jeweils verbleibende Vertragslaufzeit des bestehenden Vertrags sowie die Regelung zur Vergütung in Ziffer 3 dieser AGB.

8.2 Nachträgliche Erweiterungen gemäß Ziffer 8.1 sowie die Zuordnung bestehender Nutzerlizenzen zu höheren Lizenzklassen erfolgen über die von TROI bereitgestellten Buchungs- oder Bestellwege, insbesondere über elektronische Bestellprozesse oder individuelle Vereinbarungen in Textform.

8.3 Die Zuordnung bestehender Nutzerlizenzen zu niedrigeren Lizenzklassen sowie die Reduzierung gebuchter Nutzerlizenzen, nutzungsabhängiger Kontingente oder Nutzungspakete, gebuchter Module oder Zusatzfunktionen während der Vertragslaufzeit sind nicht möglich.

Soweit nutzungsabhängige Kontingente oder Nutzungspakete, insbesondere für Business-Actions, für einen Kalendermonat bereitgestellt werden, sind nicht verbrauchte Einheiten nicht auf nachfolgende Kalendermonate übertragbar und verfallen mit Ablauf des jeweiligen Kalendermonats; dies gilt auch für während des laufenden Kalendermonats zusätzlich, insbesondere durch automatischen oder manuellen Nachkauf, erworbene Kontingente, Nutzungspakete oder Business-Actions.

9. Pflichten des Kunden bei SaaS und Hosting

9.1 Der Kunde verwaltet die Nutzer sowie die Nutzung der SaaS-Leistungen selbst. TROI legt ausschließlich das initiale Administrator-Konto an.

9.2 Der Kunde verpflichtet sich, über die Software keine rechtswidrigen, die Gesetze, behördlichen Auflagen oder Rechte Dritter verletzenden Daten und Inhalte abzulegen.

9.3 Der Kunde ist verpflichtet, den unbefugten Zugriff Dritter auf die Software durch geeignete technische und organisatorische Maßnahmen zu verhindern, insbesondere die Zugangsdaten nicht unbefugten Dritten bekannt zu geben.

9.4 Der Kunde ist verpflichtet, seine Daten und Inhalte vor der Speicherung und Verarbeitung in der Software auf Viren oder sonstige schädliche Komponenten zu prüfen und hierzu dem Stand der Technik entsprechende Schutzprogramme einzusetzen.

9.5 Soweit an den vom Kunden im Rahmen der SaaS-Leistungen gespeicherten oder verarbeiteten Daten und Inhalten Rechte bestehen, räumt der Kunde TROI die für die Durchführung der SaaS- und Hosting-Leistungen erforderlichen Rechte ein, insbesondere zur Speicherung, Vervielfältigung, Verarbeitung, Übermittlung und Bereitstellung der Inhalte sowie zur Durchführung von Datensicherungsmaßnahmen.

9.6 Soweit der Kunde über die Software ein von ihm selbst oder von einem Dritten bereitgestelltes KI-System, Large Language Model (LLM) oder einen vergleichbaren Dienst anbindet oder von TROI gemäß dem Vertrag oder der Leistungsbeschreibung bereitgestellte KI-basierte Funktionen nutzt, ist der Kunde für die von ihm oder seinen Nutzern eingegebenen oder veranlassten Daten, Inhalte, Prompts, Vorgaben und Anweisungen verantwortlich. Der Kunde hat sicherzustellen, dass deren Eingabe, Verarbeitung und Nutzung zulässig ist und insbesondere keine Rechte Dritter, gesetzlichen Vorgaben oder vertraglichen Pflichten verletzt. KI-Systeme und KI-basierte Funktionen dürfen nicht für rechtswidrige, missbräuchliche, täuschende, diskriminierende oder sonst unzulässige Zwecke genutzt werden.

Soweit der Kunde ein von ihm selbst oder von einem Dritten bereitgestelltes KI-System, Large Language Model (LLM) oder einen vergleichbaren Dienst an die Software anbindet, ist er darüber hinaus für dessen Auswahl, Konfiguration und rechtmäßige Nutzung sowie für die hierfür erforderlichen Zugänge, Nutzungsrechte und sonstigen Berechtigungen verantwortlich.

Der Kunde hat bei der Nutzung von KI-Systemen oder KI-basierten Funktionen etwaige von TROI bereitgestellte Hinweise, Anleitungen, Nutzungsbeschränkungen und Dokumentationen zu beachten sowie die für seinen konkreten Einsatz geltenden gesetzlichen und regulatorischen Anforderungen eigenverantwortlich einzuhalten. Erkennt der Kunde erhebliche Fehlfunktionen, Sicherheitsrisiken oder sonstige Umstände, die auf eine Fehlfunktion oder nicht bestimmungsgemäße Nutzung der von TROI bereitgestellten Software, Schnittstellen oder KI-basierten Funktionen hindeuten, hat er TROI hierüber unverzüglich zu informieren und TROI bei der Prüfung und Beseitigung angemessen zu unterstützen.

9.7 Der Kunde verpflichtet sich, TROI erkennbare Störungen unverzüglich anzuzeigen und TROI bei der Fehleranalyse und Mängelbeseitigung angemessen zu unterstützen. Hierzu hat der Kunde insbesondere auftretende Probleme über das von TROI bereitgestellte Ticketsystem möglichst genau zu beschreiben, TROI die für die Fehleranalyse und Mängelbeseitigung erforderlichen Informationen und Daten zur Verfügung zu stellen und TROI angemessene Gelegenheit zur Prüfung und Mängelbeseitigung zu geben.

10. Verfügbarkeit bei SaaS und Hosting / Wartungsfenster

10.1 TROI stellt für die Erreichbarkeit der Software samt der gehosteten Daten im Jahresdurchschnitt eine Verfügbarkeit von 99% für den Zeitraum von täglich 8 Uhr bis 20 Uhr sicher.

Diese Verfügbarkeit wird an der Schnittstelle von TROI zum Internet gemessen.

Bei der Berechnung der durchschnittlichen Verfügbarkeit in Prozent wird nach kaufmännischen Grundsätzen auf eine Nachkommastelle gerundet.

10.2 Die Verfügbarkeit berechnet sich aus dem Verhältnis der tatsächlichen Verfügbarkeit der Software während der Nutzungszeiten zur vereinbarten Gesamtverfügbarkeit innerhalb des jeweiligen Betriebsjahres.

10.3 Die Ist-Zeit (IZ) ist der Zeitraum, in dem die Software während der Nutzungszeiten (täglich 8 Uhr bis 20 Uhr) an der Schnittstelle zum Internet tatsächlich für den Kunden verfügbar ist.

Die Soll-Zeit (SZ) ist die Zeit, die nach Abzug der Zeiträume, die sich aus einer Unterbrechung aus einer oder mehrerer der folgenden Ursachen ergeben, verbleibt:

- Unterbrechung aufgrund von höherer Gewalt oder anderen, nicht von TROI zu vertretenden Gründen. Hierzu gehört etwa die Unterbrechung auf Grund eines „Hacker-Angriffs“ (unerlaubter Zugriff von außen auf das System), trotz Einsatz der Sicherungsmaßnahmen;
- Unterbrechung, die aufgrund von Vorgaben des Kunden oder sonst durch ihn verursacht werden;
- Unterbrechungen infolge Unterbleibens oder verzögerter Erfüllung von Mitwirkungspflichten des Kunden;
- Unterbrechungen innerhalb der Wartungsfenster gemäß Ziffer 10.4 dieser AGB;

10.4 Als regelmäßiges Wartungsfenster werden die Zeiträume jeweils mittwochs von 3 Uhr bis 8 Uhr, mittwochs auf donnerstags von 22 Uhr bis 4 Uhr sowie samstags auf sonntags 22 Uhr bis 4 Uhr vereinbart.

Sofern die Wartung zu einem außerhalb des regelmäßigen Wartungsfensters liegenden Zeitpunkt stattfinden soll („Sonder-Wartungsfenster“), hat dies TROI dem Kunden mit einer Frist von 24 Stunden anzukündigen. Sonder-Wartungsfenster sind bei der Ist-Zeit ebenfalls nicht zu berücksichtigen. In den Wartungsfenstern finden u.a. die Wartungs- und Entstörungsmaßnahmen, Release-Wechsel, Datenbank-Reorganisation, etc. statt. TROI ist bemüht, alle Arbeiten an den Systemen möglichst ohne Beeinträchtigung des Betriebes durchzuführen.

TEIL 3: SUPPORT-LEISTUNGEN

11. Inhalt der Support-Leistungen

11.1 Während der Laufzeit des Vertrags erbringt TROI verschiedene Support-Leistungen („Support-Leistungen“), deren Umfang im Folgenden definiert ist.

11.2 Die Support-Leistungen werden als Dienstleistung nach §§ 611 ff. BGB erbracht. Ein bestimmter Erfolg ist im Rahmen der Support-Leistungen nicht geschuldet.

11.3 Die Regelungen zu den Support-Leistungen gelten nicht, soweit TROI zur gesetzlichen oder vertraglichen Mängelhaftung verpflichtet ist. Für Mängel gelten ausschließlich die Regelungen gemäß Ziffer 15 dieser AGB.

12. Umfang der Support-Leistungen

12.1 Die Support-Leistungen umfassen die Unterstützung bei Störungen oder Fehlern und zwar über ein von TROI bereitgestelltes Ticket-System.

12.2 Die Support-Leistungen beziehen sich ausschließlich auf die jeweils von TROI aktuell bereitgestellte Version der Software einschließlich der darin enthaltenen Funktionen, Module und Zusatzfunktionen.

12.3 Die Support-Leistungen beziehen sich ausschließlich auf die von TROI bereitgestellte Software. Nicht umfasst sind Supportleistungen für Drittsoftware, Fremdsysteme oder sonstige externe Komponenten, auch wenn diese über Schnittstellen oder Integrationen mit der Software verbunden sind.

12.4 Voraussetzung für die Inanspruchnahme des Supports ist eine qualifizierte Konfiguration und Nutzung der Software sowie eine entsprechende Schulung der Anwender.

12.5 Bei vom Kunden mitgeteilten Fehlern oder Störungen wird TROI versuchen, diese im Rahmen der Support-Leistungen zu beseitigen. Die Fehler- und Störungsbeseitigung kann insbesondere durch Hinweise zur Nutzung, Konfigurationsänderungen, Workarounds, Updates oder sonstige Anpassungen der Software erfolgen.

Störungen und Fehler sind vom Kunden unter möglichst genauer Beschreibung der Symptome und Auswirkungen unverzüglich über das von TROI bereitgestellte Support- oder Ticketsystem zu melden.

Für Mängel stehen dem Kunden dagegen die Mängelansprüche gemäß Ziffer 15 dieser AGB zu.

12.6 Folgende Leistungen sind nicht Bestandteil der Support-Leistungen und von TROI nur geschuldet, wenn explizit Teil des Angebots oder gesondert beauftragt: Beratung / Schulungen, Individualprogrammierungen.

TEIL 4: SCHULUNGS- UND BERATUNGSLEISTUNGEN

13. Inhalt und Umfang der Schulungs- und Beratungsleistungen

13.1 Während der Laufzeit des Vertrags erbringt TROI die im Vertrag vereinbarten Beratungs- und Schulungsleistungen im dort festgelegten Umfang.

Beratungs- und Schulungsleistungen werden als Dienstleistungen im Sinne der §§ 611 ff. BGB erbracht. Ein bestimmter Erfolg ist im Rahmen der Beratungs- und Schulungsleistungen nicht geschuldet.

13.2 Auf Anfrage des Kunden werden gemeinsam Termine für Beratungs- oder Schulungsleistungen vereinbart; von TROI bestätigte Termine sind verbindlich.

13.3 Eine Umbuchung vereinbarter Termine durch den Kunden ist bis zu 24 Stunden vor dem Termin per E-Mail möglich. Erfolgt eine Absage oder Verschiebung weniger als 24 Stunden vor dem Termin, so sind 50 % des vereinbarten Zeitaufwands zu vergüten. Soweit noch Zeit innerhalb des vereinbarten Kontingents übrig ist, darf TROI die Vergütung dieses Zeitaufwandes von dem Kontingent in Abzug bringen.

TEIL 5: WEITERE LEISTUNGEN UND ZUSATZLEISTUNGEN

14. Weitere Leistungen und Zusatzleistungen

14.1 Soweit im Vertrag weitere Leistungen genannt sind, die weder SaaS, Hosting, Support-Leistungen noch Schulungs- und Beratungsleistungen sind (kurz: „weitere Leistungen“), gilt ergänzend zu etwaigen Regelungen im Angebot dazu folgendes:

- Soweit deren Gegenstand die Herbeiführung eines bestimmten Erfolgs ist, insbesondere die Erstellung, Anpassung oder Individualisierung von Templates, Konfigurationen, Schnittstellen oder vergleichbaren Arbeitsergebnissen, gelten diese weiteren Leistungen als Werkleistungen; für sie gelten ergänzend die Regelungen der Ziffern 14.2 und 15.2.
- Soweit deren Gegenstand die Ausführung bestimmter Tätigkeiten ist, wie zum Beispiel Unterstützung bei Datenvisualisierung, gelten für diese die „Support-Leistungen“ betreffenden Regelungen dieser AGB sowie deren allgemeine Regelungen entsprechend.

14.2 Werkleistungen

Nach vollständiger Erbringung einer Werkleistung teilt TROI dies dem Kunden in Textform mit. Der Kunde hat die Werkleistung innerhalb von zwei Wochen nach Zugang der Mitteilung daraufhin zu prüfen, ob sie den vertraglich vereinbarten Anforderungen entspricht („Abnahmephase“).

Zeigen sich während der Abnahmephase wesentliche Mängel, hat der Kunde diese TROI unverzüglich, spätestens innerhalb der Abnahmephase, in Textform mitzuteilen und nachvollziehbar zu beschreiben. TROI wird ordnungsgemäß gerügte wesentliche Mängel innerhalb angemessener Frist beseitigen und dem Kunden die erneute Abnahmebereitschaft anzeigen. Die erneute Prüfung beschränkt sich auf die gerügten Mängel und etwaige durch deren Beseitigung verursachte neue Mängel.

Liegen keine wesentlichen Mängel vor oder verweigert der Kunde die Abnahme nicht innerhalb der Abnahmephase unter Angabe mindestens eines Mangels, gelten die Werkleistungen mit Ablauf der Abnahmephase als abgenommen. Unwesentliche Mängel berechtigen nicht zur Verweigerung der Abnahme.

Soweit TROI abgrenzbare Teilleistungen erbringt, kann TROI hierfür Teilabnahmen verlangen.

TEIL 6: MÄNGELANSPRÜCHE UND HAFTUNG

15. Mängelansprüche

15.1 SaaS- und Hosting-Leistungen

Bei Mängeln der SaaS- und Hosting-Leistungen richten sich die Ansprüche des Kunden nach den §§ 536 ff. BGB, soweit nachfolgend nicht anderweitig bestimmt:

TROI ist verpflichtet, Mängel der Software innerhalb angemessener Zeit zu beheben.

Soweit der Kunde ein von ihm selbst oder von einem Dritten bereitgestelltes KI-System, Large Language Model (LLM) oder einen vergleichbaren Dienst an die Software anbindet, begründen fehlerhafte, unvollständige, uneindeutige oder für den vom Kunden verfolgten Zweck ungeeignete Ergebnisse dieses Systems oder Dienstes für sich genommen keinen Mangel der Leistungen von TROI. Dies gilt nicht, soweit solche Ergebnisse auf einem Mangel der von TROI bereitgestellten Schnittstelle oder sonstigen Softwarefunktionalität beruhen.

Soweit TROI gemäß dem Vertrag oder der Leistungsbeschreibung selbst KI-basierte Funktionen als Bestandteil der Software bereitstellt, begründet die bloße inhaltliche Unrichtigkeit, Unvollständigkeit, Uneindeutigkeit oder fehlende Eignung einzelner Ergebnisse für den vom Kunden verfolgten Zweck für sich genommen keinen Mangel, soweit die KI-basierte Funktion im Übrigen dem vertraglich vereinbarten Funktionsumfang entspricht. Die verschuldensunabhängige Haftung nach § 536a Absatz 1 BGB für bereits zum Zeitpunkt des Vertragsschlusses vorhandene Fehler wird ausdrücklich ausgeschlossen.

Für Mängel, die bereits bei erstmaliger Bereitstellung der Nutzungsmöglichkeiten der Software/ des Hostings vorhanden waren, haftet TROI nur, wenn TROI diese Mängel zu vertreten hat.

Eine Kündigung des Kunden gem. § 543 II Nr. 1 BGB wegen Nichtgewährung des vertragsmäßigen Gebrauchs ist erst zulässig, wenn TROI ausreichende Gelegenheit zur Mängelbeseitigung gegeben wurde und diese fehlgeschlagen ist.

Die Mängelansprüche des Kunden gegen TROI sind ausgeschlossen, soweit der Kunde ohne Zustimmung von TROI Änderungen an der Software selbst vornimmt oder vornehmen lässt. Dies gilt nicht, sofern der Kunde zu Änderungen gesetzlich berechtigt ist, insbesondere im Rahmen der Ausübung des Selbstbeseitigungsrechts gem. § 536a Abs. 2 BGB, und die Änderungen fachgerecht ausgeführt sowie nachvollziehbar dokumentiert sind.

15.2 Werkleistungen:

Bei Mängeln von Werkleistungen stehen dem Kunden die Rechte gemäß §§ 634 ff. BGB zu, soweit nachfolgend nichts Abweichendes geregelt ist.

TROI leistet innerhalb angemessener Frist für Mängel der Werkleistungen zunächst nach eigener Wahl Nacherfüllung durch Nachbesserung oder Neuherstellung. Ist eine vollständige Mangelbeseitigung nicht möglich oder nur mit unverhältnismäßigem Aufwand verbunden, ist TROI berechtigt, dem Kunden zumutbare Fehlerumgehungsmöglichkeiten aufzuzeigen. Soweit diese dem Kunden zumutbar sind und die vertragsgemäße Nutzung nicht wesentlich beeinträchtigen, gelten sie als Nacherfüllung. Schlägt die Nacherfüllung fehl, ist sie dem Kunden unzumutbar oder wird sie von TROI endgültig verweigert, kann der Kunde nach Maßgabe der gesetzlichen Vorschriften mindern, vom Vertrag zurücktreten oder Schadensersatz statt der Leistung verlangen.

Ein Rücktrittsrecht steht dem Kunden nicht zu, wenn nur unerhebliche Mängel vorliegen. Ein Rücktritt wegen Mängeln werkvertraglicher Leistungen bezieht sich nur auf diese Leistungen.

15.3 Mängelrüge

Mängel sind gegenüber dem Anwendersupport von TROI stets unverzüglich, spätestens binnen 5 Werktagen nach Kenntniserlangung, anzuzeigen.

15.4 Verjährung

Mängelansprüche verjähren in einem (1) Jahr.

Die Verjährungsfrist beginnt mit dem gesetzlichen Verjährungsbeginn. Dies gilt jeweils nicht, wenn TROI grobe Fahrlässigkeit oder Vorsatz vorwerfbar ist, sowie im Falle von TROI zurechenbaren Körper- und Gesundheitsschäden oder bei Verlust des Lebens des Kunden oder arglistigem Verschweigen eines Mangels oder der Übernahme einer Garantie für die Beschaffenheit sowie in Fällen zwingender gesetzlicher Haftung, insbesondere nach dem Produkthaftungsgesetz.

15.5 Garantien im Rechtssinne erhält der Kunde grundsätzlich von TROI nicht, soweit dies nicht ausdrücklich schriftlich erfolgt und dabei das Wort „Garantie“ verwendet wird.

16. Haftung und Freistellung

16.1 TROI haftet unbeschränkt für Vorsatz und grobe Fahrlässigkeit sowie bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit.

Für leichte Fahrlässigkeit haftet TROI nur bei Verletzung einer wesentlichen Vertragspflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertrauen darf („Kardinalpflicht“). TROI haftet dabei nur für vorhersehbare Schäden, mit deren Entstehung typischerweise gerechnet werden muss. Im Übrigen ist die Haftung von TROI bei leichter Fahrlässigkeit ausgeschlossen.

16.2 Die Haftung von TROI bei leichter Fahrlässigkeit ist der Höhe nach je Schadensfall auf die vom Kunden für die betroffenen Leistungen in den letzten zwölf Monaten vor Eintritt des Schadensereignisses geschuldete Nettovergütung, mindestens jedoch

20.000 EUR und insgesamt höchstens 100.000 EUR pro Vertragsjahr, beschränkt. Die vorstehenden Haftungsobergrenzen begründen keinen Anspruch auf Ersatz eines über den tatsächlich ersatzfähigen Schaden hinausgehenden Betrags.

16.3 Für den Verlust von Daten und Inhalten haftet TROI nicht, soweit der Schaden darauf beruht, dass es der Kunde unterlassen hat, im Rahmen der Funktionen der Software oder anderweitig angemessene Datensicherungen vorzunehmen und dadurch sicherzustellen, dass verloren gegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

16.4 Die Parteien stellen sich wechselseitig von sämtlichen Ansprüchen Dritter und den Kosten notwendiger Rechtsverteidigung frei, die auf einer schuldhaften Verletzung von Rechten Dritter oder Gesetzesverletzungen durch die jeweils andere Partei oder ihre Erfüllungs- oder Verrichtungsgehilfen begründet sind und gegen die in Anspruch genommene Partei geltend gemacht werden. Bei der Abwehr von Ansprüchen Dritter werden die Parteien zusammenarbeiten.

16.5 Die vorstehenden Haftungsbeschränkungen gelten auch zugunsten von gesetzlichen Vertretern, Mitarbeitern und Erfüllungsgehilfen von TROI.

TEIL 7: ALLGEMEINE BESTIMMUNGEN

17. Weitere Mitwirkungspflichten des Kunden

17.1 Der Kunde wird TROI bei der Erbringung der vertraglichen Leistungen angemessen unterstützen.

Der Kunde stellt TROI insbesondere alle zur Leistungserbringung notwendigen Informationen, Daten, Unterlagen, Zugänge und sonstigen Mitwirkungen rechtzeitig zur Verfügung und erbringt vereinbarte Mitwirkungsleistungen fristgerecht.

17.2 Kommt der Kunde seinen Mitwirkungspflichten nicht nach und ist TROI hierdurch in der Leistungserbringung beeinträchtigt, verlängern sich vereinbarte Leistungsfristen angemessen. TROI ist berechtigt, hierdurch entstehenden Mehraufwand gesondert zu berechnen. Weitergehende Rechte von TROI bleiben unberührt.

17.3 Der Kunde hat die Software vor der erstmaligen produktiven Nutzung sowie nach Änderungen der Systemumgebung oder sonstigen wesentlichen Änderungen der Einsatzbedingungen auf ihre grundsätzliche Eignung für die beabsichtigte Nutzung zu überprüfen.

18. Geheimhaltung

18.1 Die Parteien verpflichten sich, sämtliche im Zusammenhang mit dem Vertrag erlangten vertraulichen Informationen sowie Betriebs- und Geschäftsgeheimnisse der jeweils anderen Partei nur zur Durchführung dieses Vertrages zu verwenden und ansonsten zeitlich unbefristet geheim zu halten.

Dies gilt gegenüber jeglichen nicht-berechtigten Dritten, d.h. auch gegenüber nicht-berechtigten Mitarbeitern, sofern eine Weitergabe solcher Informationen nicht zur ordnungsgemäßen Erfüllung der vertraglichen Verpflichtungen erforderlich ist.

Beide Parteien haben diesbezüglich auch ihre berechtigten Mitarbeiter zur Vertraulichkeit zu verpflichten.

18.2 Die Geheimhaltungspflicht gilt nicht für Informationen, hinsichtlich derer die empfangende Partei nachweist, dass die betreffenden Informationen allgemein bekannt sind, ohne Verschulden der Parteien allgemein bekannt wurden, rechtmäßig von einem Dritten erlangt wurden oder werden oder der empfangenden Partei bereits vor Offenlegung rechtmäßig bekannt sind oder aufgrund gesetzlicher Verpflichtungen oder behördlicher beziehungsweise gerichtlicher Anordnungen offengelegt werden müssen.

19. Datenschutz

19.1 Soweit TROI im Rahmen der vertraglich geschuldeten Leistungserbringung personenbezogene Daten des Kunden im Auftrag und nach dessen Weisung verarbeitet, insbesondere im Rahmen des Hostings oder soweit TROI bei Support-Zugriff Zugriff auf solche Daten erhält, erfolgt dies als Auftragsverarbeitung im Sinne des Art. 28 DSGVO.

Für Daten aus der Schweiz gelten die sich aus dem schweizerischen Recht ergebenden Anforderungen (DSV).

19.2 Die Einzelheiten der Auftragsverarbeitung sind in der Auftragsverarbeitungsvereinbarung geregelt, die als Anlage Bestandteil des Vertrags ist und mit Abschluss des Vertrags zwischen TROI und dem Kunden vereinbart wird.

20. Projektmanagement

20.1 Die Parteien benennen für die Durchführung des Vertrags jeweils einen zentralen Ansprechpartner sowie dessen Stellvertretung. Die Benennung erfolgt in Textform.

20.2 Die benannten Ansprechpartner sind berechtigt, Erklärungen im Zusammenhang mit der organisatorischen Durchführung des Vertrags entgegenzunehmen und abzugeben. Sie koordinieren die Zusammenarbeit der Parteien und sorgen dafür, dass erforderliche Entscheidungen innerhalb angemessener Zeit getroffen oder intern herbeigeführt werden.

21. Daten nach Vertragsende

21.1 Nach Beendigung des Vertrags wird TROI die im Rahmen der SaaS- und Hosting-Leistungen gespeicherten Daten des Kunden, soweit diese bei TROI noch verfügbar sind, für einen Zeitraum von 30 Tagen ausschließlich zum Abruf oder Export durch den Kunden bereithalten. Eine produktive Nutzung der Software ist während dieses Zeitraums nicht mehr geschuldet.

21.2 Für diese nachlaufende Bereithaltung gelten der Vertrag, diese AGB sowie die Auftragsverarbeitungsvereinbarung fort, soweit dies für die Bereithaltung, den Abruf, den Export, die Löschung, die Sicherheit und die Verarbeitung der Daten erforderlich ist.

21.3 TROI ist berechtigt, für die nachlaufende Bereithaltung der Daten sowie für eine vom Kunden gewünschte Unterstützung bei Datenexport, Datenmigration oder Datenübernahme eine gesonderte Vergütung nach Aufwand zu verlangen, soweit hierfür keine abweichende Vereinbarung getroffen wurde.

21.4 Nach Ablauf des vorgenannten Zeitraums ist TROI berechtigt, die Daten des Kunden zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten oder abweichenden vertraglichen Regelungen entgegenstehen. Soweit personenbezogene Daten betroffen sind, bleiben die Regelungen der Auftragsverarbeitungsvereinbarung unberührt.

22. Schlussbestimmungen

22.1 Der Kunde darf mit Forderungen gegen TROI nur aufrechnen oder ein Zurückbehaltungsrecht geltend machen, soweit seine Gegenansprüche unbestritten oder rechtskräftig festgestellt sind; Zurückbehaltungsrechte stehen dem Kunden darüber hinaus nur wegen Gegenansprüchen aus demselben Vertragsverhältnis zu.

22.2 TROI ist berechtigt, Leistungen nach diesem Vertrag auch durch Subunternehmer und andere Dritte erbringen zu lassen. Im Zusammenhang mit der Verarbeitung von personenbezogenen Daten gelten dafür vorrangig die Regelungen in der Auftragsverarbeitungsvereinbarung.

22.3 Der Kunde gewährt TROI das Recht, den Kunden als Referenz im Rahmen von Vertriebs- und Marketingaktivitäten zu benennen und in diesem Zusammenhang das Kunden-Logo zu verwenden. Der Kunde kann in Textform (z.B. per E-Mail) widersprechen.

22.4 Die Nichtausübung oder verzögerte Ausübung von Rechten aus dem Vertrag sowie die widerspruchslose Erbringung oder Entgegennahme von Leistungen, die über den vertraglich geschuldeten Leistungsumfang hinausgehen, begründen keine Änderung oder Erweiterung des Vertrags und keine Verpflichtung zur entsprechenden Leistungserbringung für die Zukunft.

22.5 TROI ist berechtigt, Rechte und Pflichten aus dem Vertrag auf verbundene Unternehmen oder im Rahmen einer Unternehmensumstrukturierung, Unternehmensveräußerung oder Übertragung des Geschäftsbereichs auf Dritte zu übertragen. Die berechtigten Interessen des Kunden bleiben unberührt.

22.6 Änderungen und Ergänzungen des Vertrags bedürfen mindestens der Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist. Die Textform wird insbesondere durch E-Mail sowie durch elektronische Signaturen oder durch die Übersendung eines unterzeichneten und eingescannten Dokuments gewahrt.

22.7 Auf diese Vereinbarung findet ausschließlich deutsches Recht Anwendung unter Ausschluss des Kollisionsrechts. Erfüllungsort und Gerichtsstand sind München, soweit gesetzlich zulässig.

22.8 Die Anwendbarkeit der Regelungen des Übereinkommens über den internationalen Warenkauf (UN-Kaufrecht) wird ausgeschlossen.

22.9 TROI ist berechtigt, diese AGB mit Wirkung für bestehende Vertragsverhältnisse zu ändern, soweit hierfür ein sachlicher Grund besteht und die Änderungen für den Kunden zumutbar sind. Ein solcher sachlicher Grund kann insbesondere bei neuen technischen Entwicklungen, der Einführung neuer Leistungen, einer Erweiterung der Funktionen oder bei Änderungen in der Rechtsprechung, Gesetzeslage oder behördlicher Vorgaben vorliegen.

TROI wird den Kunden über Änderungen mindestens sechs Wochen vor ihrem Inkrafttreten in Textform (etwa per E-Mail) informieren. Widerspricht der Kunde den Änderungen nicht innerhalb dieser Frist in Textform, gelten die Änderungen als genehmigt. Hierauf wird TROI den Kunden bei Mitteilung der Änderungen gesondert hinweisen. Im Falle eines Widerspruchs gelten die bisherigen AGB fort.

22.10 Sollten Bestimmungen des Vertrags ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder ihre Rechtswirksamkeit oder Durchführbarkeit später verlieren, soll hierdurch die Gültigkeit der übrigen Bestimmungen des Vertrags nicht berührt werden. Das Gleiche gilt, wenn sich in diesem Vertrag eine Regelungslücke herausstellen sollte. Anstelle der unwirksamen oder undurchführbaren Bestimmung oder zur Ausfüllung der Lücke soll eine angemessene Regelung gelten, die, soweit rechtlich möglich, dem am nächsten kommt, was die Parteien nach dem Sinn und Zweck der Vereinbarung gewollt hätten, sofern sie den entsprechenden Aspekt bedacht hätten.

TROI GmbH - Oktober 2026

SYSTEMVORAUSSETZUNGEN UND LEISTUNGSBESCHREIBUNG

troi aion

TEIL 1: SYSTEMVORAUSSETZUNGEN

1. Bildschirmauflösung:

Minimum:
1920x1080

2. Browser:

Chrome ab Version 155.0.8059.40

Es wird empfohlen immer die aktuelle Browser-Version zu installieren. Werbeblocker müssen deaktiviert sein.

3. Internetzugang:

Minimum: 25 Mbit/s Downloadgeschwindigkeit
Optimum: Ist abhängig von der Mitarbeiteranzahl.

TEIL 2: LEISTUNGSBESCHREIBUNG troi aion V.1.1.0

Der Funktionsumfang ist abhängig von der gebuchten Lizenzklasse der Installation (Core, Intelligence, Performance).
Die zugehörigen Funktionen der jeweiligen Lizenzklasse kann man der Übersicht in Teil 4 entnehmen.
Die Nutzung von troi aion erfolgt des Weiteren auf Basis eines kombinierten nutzungsabhängigen Modells.
Dabei werden sowohl der Verbrauch von Business-Actions für bestimmte Funktionalitäten als auch die Anzahl der ausgeführten Workflows erfasst und bewertet. Beide Faktoren können unabhängig voneinander Kosten verursachen.
Des Weiteren werden die Nutzer-Lizenzen in Full- und Time-Seat unterschieden.

1. Mitarbeiter

Im Bereich Mitarbeiter können Mitarbeiterdatensätze angelegt werden mit Vorname, Nachname, Email, Telefonnummer, Eintrittsdatum in das Unternehmen sowie einem Status.
Auf dem Reiter Feiertage & Adressen kann die Adresse und die Feiertagsregion inkl. Gültigkeit angegeben werden. Auf dem Reiter Arbeitszeit ist es möglich, dass dem Mitarbeiter ein Arbeitszeitmodell inkl. Gültigkeit eingetragen wird. Auf dem Reiter Stundensätze ist es möglich dem Mitarbeiter einen Einkaufspreis und einen Verkaufspreis pro Stunde einzutragen.
Im Reiter Urlaubsanspruch kann dem Mitarbeiter der Urlaubsanspruch eingetragen werden.

2. Benutzer

Im Bereich Benutzer können Benutzer mit Benutzernamen, E-Mail, Vornamen und Nachnamen sowie Passwort für das System angelegt werden und einem Mitarbeiter sowie einem Mandanten zugeordnet werden.

3. Kontakte

Unter Kontakte hat man die Möglichkeit Kontakte zentral anzulegen und zu verwalten. Es können die jeweiligen Kontaktdaten wie Adresse, Telefonnummer, E-Mail-Adresse und weitere Zusatzinformationen hinterlegt werden. Kontakte lassen sich über eine Suchfunktion schnell finden.
Zu jedem Kontakt können Notizen und ergänzende Informationen gespeichert werden. Zusätzlich besteht die Möglichkeit eine Historie zu führen, in der Aktivitäten wie Telefonate oder Termine dokumentiert werden können.
Kontakte können externen Systemen zugeordnet werden, indem externe Referenzen hinterlegt werden.

Die Kontaktverwaltung dient als zentrale Datenbasis für weitere Funktionen im System, um Kunden und Lieferanten zu verwalten.

4. Kunden

Ein Kunde basiert immer auf einem bereits angelegten Kontakt. Die grundlegenden Kontaktdaten werden dabei automatisch übernommen. Für jeden Kunden wird automatisch eine eindeutige Kundennummer vergeben. Kunden können in verschiedene Status unterteilt werden, wie zum Beispiel aktiv, inaktiv oder gesperrt.
Zusätzlich können kundenspezifische Informationen wie steuerliche oder organisatorische Daten hinterlegt werden.
Folgende Daten können gepflegt werden: Markenname, Globale Identifikationsnummer, Registernummer, USt-IdNr., Steuernummer, Steuerberater Name, Steuerberater USt-IdNr..

Alle Kunden können in einer Übersichtsliste eingesehen, gefiltert und bearbeitet werden.

Die Kundenverwaltung ermöglicht eine klare Trennung zwischen allgemeinen Kontakten und aktiven Geschäftspartnern im Vertrieb.

5. Lieferanten

Im Bereich Lieferanten gibt es die Möglichkeit bestehende Kontakte als Lieferanten zu definieren und zu verwalten.
Ein Lieferant basiert ebenfalls auf einem bereits angelegten Kontakt. Die grundlegenden Kontaktdaten werden automatisch übernommen.
Für jeden Lieferanten wird eine eindeutige Lieferantennummer vergeben. Zusätzlich können lieferantenspezifische Informationen hinterlegt werden. Lieferanten können in verschiedene Status unterteilt werden, wie zum Beispiel aktiv, inaktiv oder gesperrt.
Alle Lieferanten können in einer Übersichtsliste eingesehen, gefiltert und bearbeitet werden.
Die Lieferantenverwaltung dient als Grundlage für Einkaufsprozesse und die Zusammenarbeit mit externen Dienstleistern.

6. Zeiterfassung

Troi aion verfügt über ein umfassendes Zeiterfassungssystem, welches es ermöglicht Arbeitszeiten zu erfassen und diese auf verschiedene Datenentitäten im System zuzuordnen.

6.1 Kalender Zeiterfassung

In der Zeiterfassung hat man die Möglichkeit Arbeitszeiten strukturiert für ein Datum zu erfassen, darzustellen, zu bearbeiten und auszuwerten.

Die Erfassung erfolgt über einen zentralen Kalender. Die Zeiterfassungen werden in einzelnen Zeitsegmenten mit einem „von“ und einem „bis“ erfasst, somit ist es möglich den Tagesverlauf abzubilden. Diese Erfassungen können vom Nutzer angelegt, geändert oder gelöscht werden. Änderungen werden historisch nachvollziehbar gespeichert.

Die Erfassung der Segmente im Kalender kann per Drag & Drop erfolgen oder lediglich ein Fenster aufziehen. Ein Erfassungssegment (Arbeitszeit, Pause, Überstundenabbau, Reisezeit) kann in den Kalender gezogen werden und somit erfasst werden. Das Segment kann per Mausinteraktion größer und kleiner gezogen werden.
Es ist möglich parallel mehrere Segmente zu erfassen. Die erfassten Segmente bzw. Zeiten bilden die Grundlage für alle weiteren Berechnungen und Auswertungen im System.

6.2 Soll-Zeiterfassung

Sofern die Systemeinstellung aktiviert ist, können Soll-Arbeitszeiten je Mitarbeiter als Ist-Arbeitszeiten erfasst werden. Diese Funktion wird auch automatische Zeiterfassung genannt.

6.3 Verarbeitung der Zeiten

Die erfassten Zeitsegmente werden automatisch verarbeitet und in eine fachlich gültige Zeitstruktur überführt. Dabei werden die Zeiten normalisiert, zusammengeführt und nach fachlichen Regeln bewertet. Das System unterscheidet dabei nach Arbeitszeiten, Pausen und überstundenrelevanten Zeiten.
Aus den erfassten Daten entsteht eine konsistente und auswertbare Zeitbasis. Die Auswertung dieser Zeiten kann über ein Regelsystem konfiguriert werden.

6.4 Automatische Pausen

In troi aion ist es möglich eine Regelung für automatische Pausen zu hinterlegen. Dies ermöglicht es, dass nach einer bestimmten Zeit automatisch Pausenzeiten in der Erfassung hinzugefügt werden.

6.5 Überstunden

Das System führt ein Überstundenkonto pro Nutzer. Es berechnet automatisch Überstunden auf Basis der Tageswerte nach Arbeitszeitmodell. Manuelle Anpassungen (z. B. Auszahlungen oder Korrekturen) sind möglich.
Darstellung des aktuellen Überstundensaldo wird im Stundenerfassungs-Reporting angezeigt.
Überstunden werden sowohl tagesbezogen als auch als Gesamtsaldo geführt und können jederzeit ausgewertet werden.

6.6 Arbeitszeitauswertung

In der Stundenerfassung Reporting kann die Auswertung der Arbeitszeiten eingesehen werden. Es wird ein Tagessaldo, sowie ein Saldo des gewählten Zeitbereichs angezeigt. Der Zeitbereich kann maximal auf 31 Tage gewählt werden.

6.7 Zuordnung von Arbeitszeiten

Erfasste Zeiten können fachlichen Objekten (zum Beispiel Kunden, Angebote, Angebotspositionen, Projekte) zugeordnet werden, sofern diese in der Lizenzklasse enthalten sind und in den Einstellungen eingeschalten sind.
Diese Zuordnungen bleiben auch bei Änderungen der Zeiten erhalten.

6.8 Zeiterfassungen über KI

In troi aion ist es möglich Zeiterfassungen über einen KI Chat durchzuführen. Hierfür ist es notwendig, dass der Chat KI Agent korrekt konfiguriert ist. Weiter muss der System-Prompt die KI dazu befähigen, die Nutzerabsicht korrekt zu interpretieren, das geeignete troi aion Tool anhand seiner Funktion auszuwählen und auszuführen. Dabei müssen notwendige Parameter, wie z.B. der Typ der zu erfassende Zeit und das Datum deutlich sein. Die erfolgreiche Ausführung der Aktion erfolgt nur auf Bestätigung des Benutzers.

7. Berechtigungen

Berechtigungen können zentral festgelegt werden. Es kann konfiguriert werden, welche Benutzer welche Rollen haben und welche Aktionen und Daten diese im System nutzen dürfen. Es können zudem eigene Rollen angelegt und konfiguriert werden. Für jede Rolle kann festgelegt werden, ob eine Berechtigung aktiviert oder deaktiviert ist.
Berechtigungen sind hierarchisch strukturiert und unterscheiden nach read – Daten lesen, create – Daten erstellen, update – Daten ändern, delete – Daten löschen. Weiter werden Berechtigungen unterschieden nach eigenen (self) oder anderen (other) Datensätzen.

8. Preisliste

Die Preisliste dient der zentralen Verwaltung aller Leistungen, die für die Erstellung von Angeboten zur Verfügung stehen. Leistungen können mit Tags versehen werden. Für jede Leistung lassen sich Einkaufs- und Verkaufspreise, Währung und Einheiten und zusätzliche Beschreibungen eintragen. Über die Suchfunktion können vorhandene Leistungen schnell gefunden werden. Dadurch stehen allen Anwendern einheitliche und zentral gepflegte Leistungsdaten für eine effiziente Angebotserstellung zur Verfügung.

9. Währungen

Die Maske dient der Anlage und Verwaltung von Währungen, die im System für Angebote und Preisberechnungen verwendet werden. Für jede Währung werden grundlegende Stammdaten wie Name, Währungscode und Symbol hinterlegt. Zusätzlich wird der Kurs zur Systemwährung definiert, über den Beträge in die zentrale Systemwährung umgerechnet werden können. Eine Währung kann als Systemwährung festgelegt werden, wobei für die Systemwährung automatisch der Kurs 1 verwendet wird. Bereits angelegte Währungen werden in einer Übersicht.

10. Einheiten

Die Maske dient der Anlage und Pflege von Stammdaten für Einheiten, die im System beispielsweise für Leistungen, Preise und Angebote verwendet werden. Über die Schaltfläche „Neue Einheit“ wird ein Eingabedialog geöffnet, in dem die grundlegenden Informationen der Einheit erfasst werden. Dazu gehören der Name, ein Kürzel, ein optionaler Code, der Typ der Einheit sowie ein Faktor zur Umrechnung bzw. Skalierung. Bereits angelegte Einheiten werden in einer tabellarischen Ansicht mit ihren Stammdaten dargestellt.

11. Rabatte / Zuschläge

Die Rabattfunktion ermöglicht es, angebotspositionsbasierte Rabatte oder Zuschläge auf Angebotspositionen zu vergeben. Rabatte/Zuschläge können prozentual hinterlegt werden und reduzieren oder erhöhen den ursprünglichen Preis entsprechend. Die Preise der Angebotsposition, welche daraus resultieren werden automatisch berechnet und ausgewiesen. Dadurch lassen sich individuelle Preisnachlässe flexibel abbilden und bei der Angebotserstellung berücksichtigen.

12. Steuersätze

Die Funktion Steuersätze ermöglicht es, unterschiedliche Steuersätze zu verwalten und diese in Angeboten auf Positionsebene zuzuordnen. Die Steuerbeträge werden auf Basis der hinterlegten Steuersätze automatisch berechnet und in den jeweiligen Summen ausgewiesen. Dadurch können unterschiedliche steuerliche Anforderungen flexibel abgebildet und eine transparente Darstellung von Netto-, Steuer- und Bruttobeträgen gewährleistet werden.

13. Angebote

In troi aion können Angebote erstellt werden. Angebote können einem Kunden oder einem Projekt zugeordnet werden. Angebote können strukturiert und kalkuliert werden. Leistungen lassen sich als einzelne Positionen oder in Gruppen hinzufügen. Die Positionen werden mit Mengen, Einheiten, Einkaufs- und Verkaufspreisen, Rabatten und Zuschlägen versehen. Die integrierte Preisliste ermöglicht die schnelle Übernahme vorhandener Leistungen. Auf Basis der Positionen werden automatisch Summen und Margen berechnet. Das fertige Angebot kann anschließend als PDF-Dokument ausgegeben, gedruckt und weiterverarbeitet werden. Das Angebotslayout kann im Rahmen der Systemmöglichkeiten in den Angebots-Druckvorlagen angepasst werden.

14. Übersetzungen

Die Übersetzungsfunktion ermöglicht es sämtliche verwendeten Bezeichnungen innerhalb der Software anhand eines Suchmusters zu suchen und durch individuelle Begriffe zu ersetzen. Die Anpassungen können für jede verfügbare Sprache separat vorgenommen werden. Dadurch lässt sich die Software flexibel an das unternehmenseigene Wording und die individuellen sprachlichen Anforderungen anpassen, sodass eine einheitliche und vertraute Terminologie im gesamten System gewährleistet wird.

15. Prozessstatus

In troi aion gibt es die Möglichkeit einen Prozessstatus für verschiedene Datenentitäten zu definieren. Es können dabei für die folgenden Datenentitäten ein Prozessstatus definiert werden: Angebote, Mitarbeiter, Kunden, Lieferanten. Dabei können Status und Übergänge flexibel konfiguriert und durch Freigabeentscheidungen ergänzt werden. So lassen sich unternehmensspezifische Geschäftsprozesse und Genehmigungsprozesse abbilden, um transparente und nachvollziehbare Abläufe innerhalb der Software sicherzustellen.

16. Nummernkreise

Die Nummernkreisfunktion ermöglicht es, für verschiedene Datenentitäten wie Kunden, Mitarbeiter, Angebote, Angebotspositionen, Preislistenpositionen und Lieferanten sowie für Kunden- und Lieferantenkürzel individuelle angepasste Nummernkreise zu definieren. Die Vergabe der Nummern erfolgt automatisch innerhalb der jeweiligen Nummernkreise und ist durch entsprechende Mechanismen vor Nummernkollisionen geschützt. Dadurch wird eine eindeutige und konsistente Kennzeichnung der Datensätze gewährleistet und eine strukturierte Verwaltung der Unternehmensdaten unterstützt.

17. Medienbibliothek

Die Medienbibliothek ermöglicht die zentrale Ablage und Verwaltung von Dateien innerhalb der Troi Software. Dateien können Dateien hochgeladen, nach verschiedenen Kriterien gefiltert und über individuelle Freigaben gezielt für andere Benutzer sichtbar gemacht werden. Dabei lassen sich Dateien sowohl privat als auch für definierte Benutzer oder Bereiche freigeben. Der verfügbare Speicherplatz ist je nach Lizenzklasse der Instanz eingeschränkt.

18. Outlook Mail Anbindung

Troi aion ermöglicht die Anbindung eines Outlook Mailkontos, so dass System-Mails über dieses Konto aus Troi heraus versendet werden können.

19. Outlook Kalender Anbindung

Troi aion ermöglicht die Anbindung eines Outlook Kalenders, so dass Kalendereinträge im Zeiterfassungskalender von troi aion angezeigt werden können und als Zeiterfassung übernommen werden können.

20. Google Mail Anbindung

Troi ermöglicht die Anbindung eines Google Mailkontos, so dass System-Mails über dieses Konto aus Troi heraus versendet werden können.

21. Google Kalender Anbindung

Troi aion ermöglicht die Anbindung eines Google Kalenders, so dass Kalendereinträge im Zeiterfassungskalender von troi aion angezeigt werden können und als Zeiterfassung übernommen werden können.

TEIL 4: NUTZERLIZENZEN

Der Funktionsumfang einzelner Lizenzen ist abhängig von der gebuchten Nutzerlizenz (Core, Intelligence, Professional).

Pro Nutzer ist jeweils eine Nutzerlizenz nötig, um den Funktionsumfang der gewählten Lizenzklasse nutzen zu können.

Time-Seat Nutzungslizenzen sind beschränkt auf die Funktionalitäten der Zeiterfassung; Details siehe Kapitel 6.

Folgende Funktionen, Zusatzfunktionen und Schnittstellen sind in den jeweiligen ~~Nutzerlizenzen~~ Lizenzklassen enthalten:

Funktionen	Details siehe Kapitel	troi aion Core
Mitarbeiter	1.	X
Benutzer	2.	X
Kontakte	3.	X
Kunden	4.	X
Lieferanten	5.	X
Zeiterfassung	6.	X
Berechtigungen	7.	X
Preisliste	8.	X
Währungen	9.	X
Einheiten	10.	X
Rabatte/ Zuschläge	11.	X
Steuersätze	12.	X
Angebote	13.	X
Übersetzungen	14.	X
Prozessstatus	15.	X
Nummernkreise	16.	X
Medienbibliothek	17.	X
Outlook Mail Anbindung	18.	X
Google Kalender Anbindung	19.	X
Google Mail Anbindung	20.	X
Google Kalender Anbindung	21.	X
Speicherplatz		250 MB

TEIL 6: ABKÜNDIGUNGEN UND LEISTUNGSÄNDERUNGEN VON PRODUKTEN

Abkündigungen von Modulen und Teilfunktionen sind jederzeit möglich mit einem Vorlauf von 6 Monaten.

VERTRAG ZUR AUFTRAGSVERARBEITUNG / AUFTRAGSBEARBEITUNG NACH ART. 28 DSGVO, UND DSG NEU (CH)

(„AV-Vertrag")

zwischen dem

Kunden

- Verantwortlicher - nachstehend Auftraggeber genannt –

und der

Troi GmbH
Gabrielenstraße 9
80636 München

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Dieser Vertrag ist eine Ergänzung zum Hauptvertrag, der durch die Annahme des Angebots zustande kommt. Er regelt die Rechte und Pflichten von Auftraggeber und -nehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

Er begründet das Rechtsverhältnis nach Art. 28 DSGVO und, soweit anwendbar Art. 9 DSG neu CH respektive.

+ 1 Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

Bei der Verarbeitung personenbezogener Daten aus oder in der Schweiz sind die speziellen Regelungen des DSG neu CH zu beachten. Die Dienstleistung ist vom Auftraggeber in der in der EU oder Schweiz oder dem EWR zu erbringen.

In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO und, soweit anwendbar, DSG neu CH zu verstehen.

Soweit Erklärungen im Folgenden „schriftlich" zu erfolgen haben, kann dies in Form der Schriftform nach § 126 BGB erfolgen, ebenso wie durch Email-Versand des Scans des unterschriebenen Originaldokuments. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

§ 1. Gegenstand und Dauer des Auftrags

(1) Der Auftragnehmer führt die im Hauptvertrag definierten Leistungen für den Auftraggeber durch.

(2) Da der Auftragnehmer in Erfüllung seiner Aufgaben, Daten im Auftrag, nach Weisung und im Interesse des Auftraggebers verarbeitet bzw. ein Zugriff auf personenbezogene Daten bei der Auftragserfüllung nicht ausgeschlossen werden kann, erfolgt die Dienstleistung als Auftragsverarbeitung bzw. Auftragsdatenverwaltung gemäß den jeweils geltenden datenschutzrechtlichen Rechtsgrundlagen.

(3) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten im Auftrag verarbeitet.

(4) Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

§ 2. Art und Zweck der Verarbeitung

Umfang, Art und Zweck der Datenverarbeitung, die Art der Daten sowie der Kreis der Betroffenen werden in Anhang 1 beschrieben.

§ 3. Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen befugten Personen in Anhang 2.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

+ 2

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren. Zur Dokumentation wird das Troi Ticketsystem verwendet.

§ 4. Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Weisungen dokumentiert.

(3) In Eilfällen können Weisungen mündlich erteilt werden; solche Weisungen wird der Auftraggeber unverzüglich im Troi Ticketsystem nachträglich dokumentieren und bestätigen.

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

(5) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme zu kontrollieren. Vor-Ort-Kontrollen haben unter Vorankündigung von mindestens 4 Wochen und nur zu den üblichen Geschäftszeiten zu erfolgen und möglichst ohne Beeinträchtigung des Ablaufs des Auftragnehmers. Den beim Auftragnehmer anfallenden Aufwand von Kontrollen, welche die gesetzlichen Verpflichtungen überschreitet, hat der Auftraggeber dem Auftragnehmer aufwandsabhängig (Stundensatz € 180 netto zzgl. MwSt.) zu erstatten. Der Auftraggeber ist verpflichtet, alle erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 5. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen und Umfang dieses AV-Vertrags, inklusive etwaiger diesbezüglicher dokumentierter Einzelweisungen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor

der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind.

(3) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, hat der Auftraggeber zuvor schriftlich zur Vertraulichkeit nach DSGVO und, soweit anwendbar, DSG neu CH zu verpflichten.

(4) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(5) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen.

(6) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

Insofern gilt betreffend geltend gemachter Betroffenenrechte folgendes:

Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Person verantwortlich. Vor diesem Hintergrund ist der Auftragnehmer gleichwohl verpflichtet, den Auftraggeber abhängig von der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner, des Auftraggebers, Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person, das heißt bei der Beantwortung von Anfragen betroffener Personen in Bezug auf die Informationspflichten des Auftraggebers gegenüber den betroffenen Personen, deren Auskunftsrecht, ihrem Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie damit im Zusammenhang stehenden Mitteilungspflichten des Auftraggebers, dem Widerspruchsrecht oder auf automatisierte Entscheidungen einschließlich Profiling zu unterstützen, wenn die betroffene Person entsprechende Rechte geltend macht.

(7) An den Auftragnehmer gerichtete Anfragen Betroffener wird er unverzüglich an den Auftraggeber weiterleiten und nicht selbst bearbeiten oder beantworten. Der Auftragnehmer darf insbesondere während der Laufzeit dieses AV-Vertrages die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Auf Wunsch unterstützt er den Auftraggeber dabei.

+ 3 (8) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(9) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder Schweiz oder des EWR. Jegliche Verlagerung in ein Drittland darf nur unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses AV-Vertrags erfolgen.

(10) Etwaige vom Auftraggeber beim Auftragnehmer angeforderte Unterstützungsleistungen, welche die gesetzlichen Verpflichtungen überschreiten, sind dem Auftragsnehmer aufwandsbezogen mit einem Stundensatz von € 180 netto zzgl. MwSt. zu vergüten.

§ 6. Technisch-organisatorische Maßnahmen

(1) Die im Anhang 3 beschriebenen technischen und organisatorischen Datensicherheitsmaßnahmen („TOMs“) werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Der Auftraggeber hat diese vor Unterzeichnung dieser Vereinbarung geprüft und als ausreichend zum von ihm ermittelten Risiko unter Berücksichtigung der Schutzziele nach dem Stand der Technik beurteilt.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Wesentliche Änderungen sind durch den Auftragnehmer zu dokumentieren, zudem ist der Auftraggeber unverzüglich darüber zu informieren.

(3) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden. Als genehmigtes Zertifizierungsverfahren wird ein Zertifikat gem. ISO 27001 akzeptiert.

§ 7. Mitteilung bei Verletzungen / Unterstützungsleistungen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der nach Art. 28 III (f) DSGVO, insbesondere bei der Erfüllung nach den Art. 32-36 DSGVO / Art. 6, 7, 8 DSG neu CH in Verbindung mit Art. 1-5 DSV neu CH datenschutzrechtlichen Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden. Meldungen erfolgen per Email an die im Anhang 2 genannten Weisungsbefugten des Auftraggebers.

b. die Verpflichtung, dem Auftraggeber auf Aufforderung im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

c. die Unterstützung des Auftraggebers auf dessen Aufforderung für dessen Datenschutz-Folgenabschätzung.

d. die Unterstützung des Auftraggebers auf dessen Aufforderung im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, welche der Auftraggeber anfordert, welche die gesetzlichen Verpflichtungen überschreitet, die nicht ausdrücklich in der Leistungsbeschreibung des Hauptvertrags aufgenommen oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung nach Aufwand (Stundensatz € 180 netto zzgl. MwSt.) beanspruchen.

§ 8. Unterauftragsverhältnisse

(1) Der Auftragnehmer darf sich bei der Leistungserbringung Subunternehmer bedienen. Die in Anhang 2 aufgelisteten Subunternehmer des Auftragnehmers sind genehmigt.

(2) Falls der Auftragnehmer einen Subunternehmer ersetzen oder einen zusätzlichen Subunternehmer einschalten möchte, wird er den Auftraggeber darüber informieren. Der Auftraggeber ist sodann berechtigt, binnen dreißig (30) Tagen nach Erhalt der Mitteilung gegen die Unterbeauftragung Einspruch beim Auftragnehmer einzulegen, was schriftlich erfolgen muss. Erfolgt dies nicht, hat der Auftraggeber den jeweiligen Unterauftragnehmer genehmigt. Erfolgt dagegen ein Einspruch und liegen für diesen nachvollziehbare Gründe vor, wird der Auftragnehmer wirtschaftlich sinnvolle Anstrengungen unternehmen, um die Leistung zu erbringen, ohne den neuen Unterauftragnehmer einzuschalten. Ist ihm dies nicht möglich, ist der Auftraggeber berechtigt, den AV-Vertrag durch schriftliche Mitteilung an den Auftragnehmer unter Einhaltung einer Frist von 30 Tagen außerordentlich zu kündigen. Alternativ kann der Auftragnehmer dem Auftraggeber einen anderen Subunternehmer vorschlagen; für diesen Fall gelten die Regelungen des vorstehenden Unterabsatzes entsprechend. Nach vorstehenden Regelungen zulässige Unterauftragnehmer hat der Auftragnehmer in Anhang 2 aufzunehmen und dem Auftraggeber als aktualisierte Fassung zu übersenden.

+ 4

(3) Der Auftragnehmer hat seine AV-Verträge mit Subunternehmern so zu gestalten, dass den Anforderungen des Art. 28 DSGVO / Art. 6, 7, 8 DSG neu CH in Verbindung mit Art. 1-5 DSV neu CH entsprechen. Erst im Anschluss darf der Auftragnehmer personenbezogene Daten des Auftraggebers dem Subunternehmer weiterleiten.

(4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(5) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder Schweiz oder des EWR erbringen, ist dem Auftragnehmer nur bei Beachtung der Art. 44 ff DSGVO/ Art. 6, 7 DSG neu CH gestattet. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

(6) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers angemessen zu überprüfen und zu dokumentieren. Auf Aufforderung hat der Auftragnehmer dem Auftraggeber die Dokumentation vorzulegen.

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

§ 9. Beendigung des AV-Vertrags / Löschung und Rückgabe von personenbezogenen Daten

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer alle im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu löschen oder in Form einer aktuellen Datenbank-Kopie an den Auftraggeber zu übergeben.

Ebenfalls zu löschen sind sämtliche vorhandene Kopien der Daten.

Die Löschung hat jeweils so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer ist verpflichtet, die Rückgabe bzw. Löschung nach Abs. (1) auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber auf Aufforderung vorzulegen.

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

§ 10. Haftung

Soweit im Hauptvertrag keine Regelungen zur Haftung enthalten sind, gelten für die Haftung des Auftragnehmers im Rahmen dieses AV-Vertrags die gesetzlichen Haftungsregelungen, ansonsten die Haftungsregelungen im Hauptvertrag entsprechend.

§ 11. Sonstige Bestimmungen

(1) Soweit die Daten beim Auftragnehmer durch Beschlagnahme oder Pfändung, durch ein Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer hat alle in diesem Zusammenhang Beteiligten zu informieren, dass ausschließlich der Auftraggeber Verantwortlicher und „Herr der Daten“ ist.

(2) Nebenabreden müssen in schriftlicher oder elektronisch dokumentierter Form (z.B. E-Mail) unter Bezugnahme auf diesen Vertrag getroffen werden. Dasselbe gilt für Änderungen und Ergänzungen dieses Vertrags. Diese müssen die geänderte Regelung ausdrücklich bezeichnen.

(3) Für den AV-Vertrag gilt das Recht der Bundesrepublik Deutschland, soweit nicht die DSGVO vorrangige Regelungen enthält. Soweit im Hauptvertrag ein Gerichtsstand vereinbart wurde, gilt diese Vereinbarung auch für alle Ansprüche oder Angelegenheiten, die sich aus oder im Zusammenhang mit diesem AV-Vertrag ergeben.

(4) Sollten einzelne Teile dieses AV-Vertrags unwirksam sein, so berührt dies die Wirksamkeit des AV-Vertrags im Übrigen nicht. Bei Vorliegen einer unwirksamen Regelung oder eine Lücke sind diese durch die Regelung zu ersetzen, die die Parteien in Kenntnis der Unwirksamkeit oder der Lücke vereinbart hätten und die der fehlerhaften Regelung möglichst nahekommt.

+ 5

§ 12. Anlagen

Anhang 1: Details zur Auftragsverarbeitung

Anhang 2: Weisungsbefugte Personen, genehmigte Subunternehmer

Anhang 3: technische und organisatorische Maßnahmen

Anhang 1 zum Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung:

Auflistung der beauftragten Dienstleistungen (Umfang, Art, Zweck der Verarbeitung, Art der Daten, Kreis der Betroffenen)

1	2	3	4	5
Lfd. Nr.	**Kurzbeschreibung der Leistungen/ Services, die der AN für den AG erbringt** (In Kurzform)	**Gegenstand, Art und Zweck der diesbezüglichen Verarbeitung von personenbezogenen Daten** (welche Leistungen betreffend die personenbezogenen Daten sind im Einzelnen zu erbringen: Erheben? Speichern? Übermitteln? Wie? Etc.)	**Kreis der Betroffenen** (=die Personengruppen, deren Daten verarbeitet werden) (Beispiele: Mitarbeiter des AG, Endkunden des AG, Azubis des AG, etc.)	**Art der personenbezogenen Daten, die der AN erhält/ verarbeitet** (=Kategorie der Daten, wie etwa „Adressdaten“ oder „Bestelldaten“, etc.
1 + 6	Bereitstellung der Funktionalitäten der TROI Software per Software-as-a-Service	Verarbeitung derjenigen personenbezogenen Daten, die der AG in der TROI Software speichert sowie bei deren Betrieb anfallen, zur jeweiligen softwareseitigen Funktionsbereitstellung und -durchführung	**Stets der Fall:** - Auftraggeber - Nutzer der TROI Software, v.a. Mitarbeiter des Auftraggebers **Je nachdem, welche Daten der Auftraggeber in der TROI Software selbst speichert und verarbeitet:** z.B. Kunden des Auftraggebers, Lieferanten des Auftraggebers, Geschäftspartner des Auftraggebers	**Daten betreffend den Auftraggeber** - Firma und Kontaktdaten - Vertragsabrechnungs- und Zahlungsdaten, Kommunikationsdaten **Daten der Nutzer, also in der Regel Mitarbeiter des Auftraggebers** - Account Daten, v.a. zur Authentifizierung und Autorisierung der Nutzer - Nutzungsdaten, insbesondere in Form von Logfiles: IP Adressen in Logfiles und der Firewall, abgerufene Funktionen **In der Software TROI vom Auftraggeber gespeicherte Daten, z.B.:** - alle personenbezogenen Daten, die der Auftraggeber in der TROI Software speichert, z.B. - die eigenen Kundendaten des Auftraggebers (Stammdaten, Kommunikationsdaten, etc.) - Projektdaten, wie zum Beispiel Abwesenheiten, Kalendereinträge, Zeiterfassungsdaten, etc.
2	User Help Desk zur Unterstützung bei Softwarestörungen und Softwarefehlern (1st Level-Support,	Verarbeitung derjenigen personenbezogenen Daten, die der Auftraggeber bzw. der jeweilige Ticketersteller im Ticketsystem bereitstellt und bei dessen Nutzung anfallen,	**Stets der Fall:** - Auftraggeber - Nutzer der TROI Ticketsystems, v.a. Mitarbeiter des Auftraggebers	**Daten betreffend den Auftraggeber** - Kontaktdaten im Rahmen der Erbringung des Supports

	2nd Level -Support, 3rd Level -Support	zur Bearbeitung der jeweiligen Problemstellung	**Je nachdem, welche Daten der Auftraggeber im Ticket angibt**: z.B. Kunden des Auftraggebers, Lieferanten des Auftraggebers, Geschäftspartner des Auftraggebers	- Mails im direkten Geschäftsverkehr oder im Rahmen von Supportleistungen **Im Ticketsystem vom Auftraggeber gespeicherte Daten, z.B.:** - Name und Kontaktdaten des Ticketerstellers, also in der Regel eines Users der Software - alle personenbezogenen Daten, die der Ticketersteller im Ticketsystem speichert oder bei Bearbeitung des Tickets anfallen (das gemeldete Problem, Emails dazu, Telefonate, technische Angaben, etc.)
3	Schulungs-/Beratungsleistungen zur TROI Software und oder den Prozessen des Auftraggebers	Verarbeitung derjenigen personenbezogenen Daten, die zur Organisation und Durchführung der Schulung sowie zur Erbringung der gewünschten Beratungsleistung erforderlich sind oder im Rahmen der Durchführung anfallen	**Stets der Fall:** - Auftraggeber - Teilnehmer der Schulung / Beratung, v.a. Mitarbeiter des Auftraggebers	**Daten betreffend des Auftraggebers** - Kontaktdaten im Rahmen der Schulung - Mails im direkten Geschäftsverkehr - Angaben zur beauftragten Schulung/ Beratung (Zeitpunkt, Ort, Inhalte, etc.) **Daten der Teilnehmer** - Name, berufliche Kontaktdaten, Angaben zur gewünschten Schulung - Teilnahmedaten (Teilnahme, etc.)

+ 7

Anhang 2 zum Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung:

Liste der weisungsbefugten Personen des Auftraggebers

Die Weisungen des Auftraggebers werden durch die jeweils dazu berechtigten Rollen bzw. Funktionen erteilt. Eine namentliche Nennung der Personen erfolgt nicht; maßgeblich ist die Zuweisung der entsprechenden Funktion beim Auftraggeber. Der Auftraggeber teilt dem Auftragnehmer die konkret mit diesen Rollen betrauten Personen auf Verlangen oder bei wesentlichen Änderungen in Textform mit.

Funktion	Bereich / Abteilung	Umfang der Weisungsbefugnis
Geschäftsführung / Vorstand	Unternehmensleitung	Uneingeschränkt (strategisch und operativ)
Datenschutzbeauftragte/r	Datenschutz / Compliance	Fachspezifisch (Datenschutzbestimmungen, Audits)
Abteilungsleitung Fachabteilung	Entsprechende Abteilung	Bereichsspezifisch
Projektleitung	Projektmanagement	Projektbezogen

Liste der Ansprechpartner des Auftragnehmers

Troi GmbH

Gabrielenstraße 9

80636 München

Name	Position	Telefon	E-Mail-Adresse
Götz, Kerstin	Geschäftsführerin	+49 (0)89 30905195-0	k.goetz@troi.de
Schad, Martin	CTO / Interner Datenschutzkoordinator	+49 (0)89 30905195-0	datenschutz@troi.de

+ 8

Liste der Subunternehmer des Auftragnehmers

Name	Anschrift	Beschreibung	Telefon	E-Mail-Adresse
Atlassian Pty Ltd	Level 6, 341 George St, Sydney NSW 2000, Australia	Dokumentation, Ticketing (EU Server)	+61 2 9262 1443	privacy@atlassian.com
Digimagical GmbH	Legstattgasse 4-6/C25 3001 Mauerbach Österreich	Hosting	+43 720 343873	office@digimagical.com
Google Ireland Limited	Gordon House, Barrow Street, Dublin4, Irland	Bereitstellung und optimierte Darstellung von Webschriftarten (Fonts)	+353 1 436 1000	Google Datenschutz-Supportformular
HubSpot Germany GmbH	Am Postbahnhof 17, 10243 Berlin	Kundenkommunikation	+49 30 217998000	hubspotgermany@hubspot.com
Stripe Payments Europe, Limited	The One Building, 1 Lower Grand Canal Street, Dublin 2, Ireland	Abwicklung von Online-Zahlungen, Kreditkartenprocessing, Abrechnung	/	privacy@stripe.com

Alle Serverstandorte der oben genannten Subunternehmer befinden sich in der EU.

+ 9

Anhang 3 zum Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung:

Technisch-organisatorische Sicherheitsmaßnahmen **für Support**

1. Zutrittskontrolle

A.	Serverseitig getroffene Zutrittskontrollmaßnahmen
1.0	Werden die Auftragsdaten des Auftraggebers auf von Ihnen oder in Ihrem Auftrag betriebenen Servern physikalisch gespeichert? x ja ☐ nein
	Wenn 1.0 nein: In diesem Fall müssen Sie die Fragen 1.1 bis 1.29 nicht beantworten. Bitte gehen Sie dann gleich zu Frage 1.30 über! Auch die Fragen 7.1 bis 7.20 entfallen.
1.1	Nennen Sie bitte die genaue Adresse des Standorts des Serverraums / Rechenzentrums (RZ). Adresse des Serverstandortes: Nessus, Fernkorngasse 10, 1100 Wien
1.2	Sind die Auftragsdaten auf mehr als einen Serverstandort / Rechenzentrum verteilt (z. B. Backup Server/ Nutzung von Cloud-Dienstleistungen)? x ja ☐ nein
1.3	Falls 1.2 ja: Machen Sie bitte die entsprechenden Adressangaben auch bzgl. weiterer Server. Weitere Serverstandort: Nessus, Dampfgasse, 1100 Wien
1.4	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für alle im Einsatz befindlichen Server- / RZ Standorte? x ja ☐ nein
1.5	Falls 1.4 nein: Beantworten Sie bitte die Fragen 1.6 bis 1.29 und 7.1 bis 7.20 für weitere RZ- / Serverstandorte.
1.6	Wird der Server / das RZ durch Sie (AN) selbst, oder durch einen Dienstleister / Subunternehmer betrieben? ☐ Auftragnehmer x Dienstleister
1.7	Sofern der Server durch einen Subunternehmer betrieben wird, nennen Sie bitte Namen und Sitz des Dienstleisters Digimagical GmbH, Legstattgasse 4-6/C25, 3001 Mauerbach, Österreich
1.8	Im wievielten Stock steht der Server, auf dem die Auftragsdaten gespeichert werden? ☐ EG ☐ Keller x 1. OG
1.9	Ist der Serverraum fensterlos? x☐ ja ☐ nein
1.10	Wenn 1.9 nein: Wie sind die Fenster vor Einbruch geschützt? ☐ vergittert ☐ alarmgesichert ☐ abschließbar ☐ gar nicht ☐ Sonstiges: bitte eintragen
1.11	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? x ja ☐ nein
1.12	Wenn 1.11 ja: Wer wird informiert, wenn die EMA auslöst? Mehrfachantworten möglich! x beauftragter Wachdienst x Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
1.13	Ist der Serverraum mit einem elektronischen Schließsystem versehen? x ja ☐ nein
1.14	Wenn 1.13 ja: Welche Zutrittstechnik kommt zum Einsatz? Mehrfachantworten möglich! x RFID ☐ PIN x Biometrie ☐ Sonstiges: bitte eintragen

+ 10

1.15	Wenn 1.13 ja: Sind die Zutrittstechniken personenbezogen vergeben / personifiziert? x ja ☐ nein
1.16	Wenn 1.13 ja: Werden die Zutritte zum Raum im Zutrittssystem gespeichert/protokolliert? x ja, sowohl erfolgreiche / positive, als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche / positive Zutritte ☐ nein, das Schloss wird nur freigegeben oder nicht
1.17	Wenn 1.16 ja: Wie lange werden die Zutrittsdaten ungefähr gespeichert? 30 Tage
1.18	Existiert ein mechanisches Schloss? ☐ ja x nein
1.19	Wenn 1.18 ja, wie viele Schlüssel zum Serverraum existieren und wo werden diese aufbewahrt. Anzahl Schlüssel: Aufbewahrungsort:
1.20	Wenn 1.18 ja: Wird die Schlüsselausgabe protokolliert? ☐ ja ☐ nein
1.21	Wenn 1.18 ja: Wie wird protokolliert und wer gibt die Schlüssel aus? ☐ Schlüsselbuch Ausgabestelle:
1.22	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Siehe Anhang 2 (Ansprechpartner Digimagical)
1.23	Ist der Serverraum videoüberwacht? x ja ☐ nein
1.24 **+ 11**	Wenn 1.23 ja: Wie lange werden die Bilddaten gespeichert? 30 Tage
1.25	Wie ist der Zutritt durch betriebsfremde Personen zum Serverraum geregelt? (bspw. Im Falle von Wartungsdiensten / Elektrikern / Reinigungspersonal). ☐ es gibt keine Regelung x Zutritt & Anwesenheit nur in Begleitung ☐ Sonstiges: bitte eintragen
1.26	Werden Zutritte durch Betriebsfremde zum Serverraum protokolliert? x ja ☐ nein
1.27	Aus welchem Material besteht die Zugangstür zum Serverraum? x Stahl / Metall ☐ sonstiges Material
1.28	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt? ☐ ja x nein
1.29	Wenn 1.28 ja: Was wird in dem Serverraum noch aufbewahrt? ☐ Telefonanlage ☐ Lagerung Büromaterial ☐ Lagerung Akten ☐ Archiv ☐ Lagerung von IT Ausstattung ☐ Sonstiges: Verteilerraum / Sicherungen / Telefonleitungen

B.	Clientseitig getroffene Zutrittskontrollmaßnahmen
1.30	Nennen Sie bitte die genaue Adresse des Standorts der Clientarbeitsplätze, von denen auf die Auftragsdaten zugegriffen wird. Troi GmbH, Gabrielenstraße 9, 80636 München, Deutschland Digimagical GmbH, Fernkorngasse 10/Stiege 3/DG in 1100 Wien, Österreich (Details siehe Anhang 4)

1.31	Ist das Bürogebäude vollständig umfriedet (Zaun, Mauer o.ä.). ☐ ja x nein
1.32	Im wievielten Stock befinden sich die Büroräume? ☐ EG ☐ Keller ☐ im gesamten Gebäude x im 3. OG
1.33	Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros? ☐ ja x nein
1.34	Wird ein Besucherbuch geführt? ☐ ja x nein
1.35	Ist das Gebäude / die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja x nein
1.36	Wenn 1.35 ja: Wer wird informiert, wenn die EMA auslöst? ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
1.37	Ist das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen? x ja, Gebäude und Büroräume sind elektronisch verschlossen ☐ ja, aber nur das Gebäude, nicht der Eingang zu den Büros / zur Büroetage. ☐ ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt. ☐ nein
1.38	Wenn ja 1.37: Welche Zutrittstechnik kommt zum Einsatz? Mehrfachantworten möglich! x NFC ☐ PIN ☐ Biometrie ☐ Sonstiges: bitte eintragen
1.39	Wenn 1.37 ja: Sind die Zutrittstechniken personenbezogen vergeben / personifiziert? x ja ☐ nein
1.40 **+ 12**	Wenn 1.37 ja: Werden die Zutritte im Zutrittssystem gespeichert/protokolliert? x ja, sowohl erfolgreiche / positive, als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche / positive Zutritte ☐ nein, das Schloss wird nur freigegeben oder nicht.
1.41	Wenn 1.40 ja: Wie lange werden die Zutrittsdaten ungefähr gespeichert? Letzten 1000 Zutritte
1.42	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? x ja ☐ nein
1.43	Wird die Ausgabe von Schlüsseln protokolliert und wer gibt die Schlüssel aus? ☐ nein, die Ausgabe wird nicht protokolliert x ja, die Ausgabe wird mittels eines Formulars / Schlüsselbuch dokumentiert. Ausgabestelle ist: Martin et Karczinski GmbH/Troi GmbH
1.44	Ist das Bürogebäude, bzw. seine Zugänge videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung x nein
1.45	Wenn 1.44 „ja, mit Bildaufzeichnung“, wie lange werden die Bilddaten gespeichert?

C.	Generelle Maßnahmen

1.46	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher; Fremdpersonal) zu den Büroräumen? ☐ nein x ja, betriebsfremde Personen werden am Eingang / Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.

2. Zugangskontrolle

2.1	Existiert ein persönlicher Passwort / (PW) Benutzername Zugangsschutz zu den Systemen, mit denen die Auftragsdaten verarbeitet werden? x ja ☐ nein
2.2	Wie werden die Zugangsberechtigungen vergeben? x auf Antrag (schriftlich oder Mail) an IT x Antrag muss durch Vorgesetzten genehmigt sein ☐ Sonstige Vergabeweise: bitte angeben
2.3	Existiert für die Administration der Systeme ein eigenständiger ADMIN-Account, der sich von seinem eigentlichen User-Account des Admins unterscheidet? x ja ☐ nein, der Admin benutzt die Systeme immer als angemeldeter ADMIN
2.4	Existieren verbindliche Passwortparameter im Unternehmen? x ja ☐ nein
2.5 + 13	Wie lauten die Passwort (PW) Vorgaben: PW Länge: x 8 Zeichen oder mehr ☐ Weniger als 8 Zeichen ☐ Weniger als 6 Zeichen Welche Zeichenarten müssen erfüllt sein? x Sonderzeichen x Ziffern x Groß- / Kleinschreibung Gültigkeitsdauer des PW: ☐ 90 Tage oder weniger ☐ 180 Tage oder weniger x mehr als 180 Tage
2.6	Nach wie vielen Zyklen darf ein Nutzer dasselbe PW frühestens erneut vergeben (Passworthistorie)? x keine Vorgabe ☐ 1 - 2 Zyklen ☐ 3 – 5 Zyklen ☐ mehr als 5 Zyklen
2.7	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben? x ja ☐ nein
2.8	Ist eine automatische PW geschützte Bildschirmsperre eingestellt? x ja ☐ nein
2.9	Wenn 2.8 ja, Nach wie vielen Minuten der Inaktivität aktiviert sich die Bildschirmsperre? 5 Minuten
2.10	Existieren verbindliche Vorgaben zum manuellen Sperren des Clients beim Verlassen des Arbeitsplatzes? x ja, der Rechner ist manuell zu sperren ☐ nein
2.11	Kontrollieren Sie die Aktualität der Zugangsberechtigungen? x ja, regelmäßig ☐ nein, nur im Falle eines konkreten Anlasses
2.12	Welche Maßnahmen ergreifen Sie bei Verlust / Vergessen / Ausspähen eines PW? x Admin setzt neues PW, das der Nutzer dann nach Erstanmeldung zu ändern hat ☐ keine

2.13	Gibt es eine Begrenzung von Anmeldeversuchen mit einem Benutzernamen / PW? x ja ☐ nein
2.14	Wenn 2.13 ja, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre durch die IT gesperrt x Die Zugänge bleiben für einen gewissen Zeitraum gesperrt (Steigerung des Zeitraums pro Fehlversuch).
2.15	Bei Fernzugängen (VPN / IPSec): Mehrfachantworten möglich! Authentisierung mit x pre-shared key x Zertifikat PW Länge: x 8 Zeichen oder mehr ☐ Weniger als 8 Zeichen ☐ Weniger als 6 Zeichen Welche Zeichenarten müssen erfüllt sein? x Sonderzeichen x Ziffern x Groß- / Kleinschreibung Gültigkeitsdauer des PW: ☐ 90 Tage oder weniger ☐ 180 Tage oder weniger x mehr als 180 Tage
2.16	Gibt es eine Begrenzung von Anmeldeversuchen bei Fernzugängen? x ja ☐ nein
2.17	Wenn 2.16 ja, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre durch die IT gesperrt x Die Zugänge bleiben für 30 Minuten gesperrt.
2.18	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? x ja ☐ nein
2.19 **+ 14**	Wie viele MA haben über Fernzugänge Zugang auf die Daten des AG? Alle Personen beschränkt über Berechtigungskonzept. Läuft der Zugang über die Fernzugänge über ☐ Sammelkennung x individuelle Einzelkennung
2.20	Werden die Systeme, auf denen die Daten des Auftraggebers verarbeitet werden, über eine Firewall abgesichert? x ja ☐ nein
2.21	Wenn 2.20 ja: Wird die Firewall regelmäßig upgedatet? x ja ☐ nein
2.22	Wenn 2.20 ja: Wer administriert Ihre Firewall? ☐ eigene IT x Externer Dienstleister
2.23	Wenn ein externer DL zum Einsatz kommt: Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten? x ja ☐ nein, die Aufschaltung ist nur im 4 Augenprinzip mit einem Mitarbeiter der eigenen IT möglich.
2.24	Wenn ein externer DL zum Einsatz kommt: Haben Sie einen Vertrag zur Auftragsdatenverarbeitung mit diesem abgeschlossen? x ja ☐ nein

3. Zugriffskontrolle

3.1	Existiert ein differenzierendes Berechtigungskonzept, das den Zugriff Ihrer Mitarbeiter auf die Daten des Auftraggebers regelt? x ja ☐ nein
3.2	Wie werden die Zugriffsberechtigungen Ihrer Mitarbeiter auf die Daten des Auftraggebers vergeben? Mehrfachantworten möglich! x auf Antrag (schriftlich oder Mail) an IT x Antrag muss durch Vorgesetzten genehmigt sein
3.3	Wie wird gewährleistet, dass die Zugriffsberechtigungen bei Abteilungs- / Funktionswechsel und / oder Ausscheiden eines Mitarbeiters aktualisiert / entzogen werden? Mehrfachantworten möglich! x personelle Veränderungen werden der IT Abteilung durch die Personalabteilung gemeldet. ☐ die zuständigen Vorgesetzten haben personelle Änderungen in ihrer Abteilung an die IT zu melden. ☐ Die Berechtigungen werden nach Art der Änderungen / des Wechsels angepasst bzw. entzogen. ☐ Sonstiges: bitte angeben
3.4	Werden Vergabe / Änderungen von Zugriffsberechtigungen protokolliert? x ja ☐ nein
3.5	Existieren getrennte Produktiv- und Testsysteme im Falle der Notwendigkeit der Wartung der Systeme? ☐ ja x nein
3.6	Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten, CD-ROMs, DVDs / Disketten), auf denen Auftragsdaten gespeichert sind, in Ihrem Unternehmen entsorgt? x Physikalische Zerstörung durch eigene IT. ☐ Physikalische Zerstörung durch externen Dienstleister. ☐ Sonstiges: bitte angeben
3.7 + 15	Wie werden nicht mehr benötigte Unterlagen mit personenbezogenen Daten des Auftraggebers (bspw. Ausdrucke / Akten / Schriftwechsel) in Ihrem Unternehmen entsorgt? ☐ Altpapier / Restmüll x Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist. ☐ Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden. x Sonstiges: Der verwendete Schredder entspricht der Sicherheitsstufe 4.
3.8	Wenn bei Ziff. 3.7 ein externer DL zum Einsatz kommt: Haben Sie einen Vertrag zur Auftragsdatenverarbeitung mit diesem abgeschlossen? ☐ ja ☐ nein
3.9	Dürfen Ihre MA eigene Speichermedien (z.B. USB Sticks) verwenden? ☐ generell ja ☐ ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT. x nein, alle benötigten Speichermedien werden vom Unternehmen gestellt.

4. Weitergabekontrolle

4.1	Wie erfolgt der Datentransfer zwischen Ihnen und dem AG? Mehrfachantworten sind möglich! x Webportal x mobiler Datenträger x E-Mail (Text und Anhänge wie PDF- / Excel- / Worddateien) ☐ Fax x Schriftlich x telefonisch x FTP Server ☐ Share Point

	x Einsichtnahme am Monitor (bspw. Fernwartung per Teamviewer, Zoom, MS Teams o.ä.) ☐ Sonstiges (z.B. Clouddienste wie Drop Box): bitte angeben
4.2	Wenn die Daten elektronisch übertragen werden, erfolgt dieser Transfer verschlüsselt / technisch geschützt? ☐ nein (z.B. http / FTP) ☐ nein, aber persönliche Übergabe (bspw. Ausdrucke, Speichermedien wie bspw. DVDs) x ja, per PW geschütztem ZIP Archiv / PDF / Excel File als Mailanhang ☐ ja, per PGP ☐ ja, per verschlüsselten Datenträger ☐ ja, per verschlüsseltem VPN x ja, per https / SSL x ja, per SFTP ☐ ja, Sonstiges: bitte angeben
4.3	Gibt es eine Vereinbarung, welche Personen auf Seite des AG und des AN die Daten übertragen dürfen? x ja ☐ nein
4.4	Wenn 4.3 ja: Wer ist jeweils zur Übertragung von Auftragsdaten befugt? AG: siehe Weisungsbefugte Anhang 2 AN: Alle Mitarbeiter nach Berechtigungskonzept
4.5	Werden die Übertragungsvorgänge protokolliert? x ja ☐ nein
4.6	Werden Auftragsdaten des AG durch Ihr Unternehmen (bzw. Ihre Mitarbeiter) auch auf mobilen Endgeräten verarbeitet? x ja ☐ nein
4.7	Wenn 4.6 ja: Wie sind die Endgeräte bzw. die darauf gespeicherten Auftragsdaten bei der Übertragung gesichert? Mehrfachantworten sind möglich! ☐ außer dem Schutz durch die allgemeine PW / Benutzerkennung keine weiteren Maßnahmen. x Verschlüsselung der Festplatten / Verzeichnisse gem. modernen Standards x über eine VPN-Verbindung zum eigenen Firmennetz ☐ über eine VPN-Verbindung zum Auftraggeber x Sonstiges: Der verwendete Schredder entspricht der Sicherheitsstufe 4.
4.8	Wenn 4.6 ja: Verarbeiten Ihre Mitarbeiter Auftragsdaten des AG auch auf eigenen privaten Geräten (bring your own device)? ☐ ja x nein
4.9	Können Ihre Mitarbeiter auf die Daten des Auftraggebers vom Home-Office aus zugreifen. x ja ☐ nein x Sonstiges: Für Arbeiten im Home-Office oder von unterwegs werden ausschließlich dienstliche Endgeräte genutzt. Verbindungen in das Rechenzentrum werden ausschließlich über VPN ermöglicht. Der Einsatz privater Geräte ist verboten.

+ 16

5. Eingabekontrolle

5.1	Werden Zugriffe (Lesen, Änderungen, Löschen) auf Daten des Auftraggebers personenbezogen protokolliert? x ja ☐ nein
5.2	Wenn 5.1 ja: Wie lange werden diese Protokolldaten aufbewahrt? 90 Tage
5.3	Wenn 5.1 ja: Werden die Protokolle ausgewertet? ☐ ja x nein, eine Auswertung wäre aber im Bedarfsfall möglich
5.4	Wenn 5.1 nein: Ist zumindest der letzte Zugriff auf die Daten (Uhrzeit / Datum der Änderung) feststellbar? ☐ ja ☐ nein

6. Auftragskontrolle

6.1	Hat Ihr Unternehmen schriftlich einen fachkundigen Datenschutzbeauftragten (DSB) bestellt? ☐ ja, interner DSB (Mitarbeiter des Auftragnehmers) x ja, externer DSB ☐ nein
6.2	Wenn 6.1 ja: Nennen Sie bitten den Namen und Kontaktdaten Ihres DSB. IITR Datenschutz GmbH Dr. Sebastian Kraska Marienplatz 2 80331 München E-Mail: email@iitr.de Telefon: +49 (089) 18917360 Impressum: https://www.iitr.de/unternehmen/impressum.html
6.3	Wenn 6.1 ja: Welche nachweisbare Qualifikation besitzt der bestellte DSB? ☐ keine ☐ nachweisbare Lehrgangsteilnahme zum Datenschutzbeauftragten (bspw. beim TÜV, IHK o.ä.) x es handelt sich um einen Juristen ☐ es handelt sich um einen Informatiker ☐ Sonstige Qualifikation: bitte angeben
6.4	Werden Ihre MA, die Auftragsdaten verarbeiten, nachweislich im Datenschutzrecht geschult? ☐ ja, Präsenzschulungen ☐ ja, eLearning x Merkblätter / Handouts ☐ nein
6.5	Werden Ihre MA schriftlich auf das Datengeheimnis verpflichtet? x ja ☐ nein
6.6	Werden Ihre MA (soweit erforderlich) schriftlich auf das Sozialgeheimnis verpflichtet? ☐ ja x nein
6.7	Setzen Sie zur Erfüllung Ihrer Pflichten aus dem Vertrag mit dem AG auch weitere Subunternehmer ein? x ja ☐ nein
6.8	Sind die von Ihnen eingesetzten Subunternehmer dem AG gegenüber benannt worden und vom AG genehmigt? x ja siehe Anhang 2 ☐ nein, bisher noch nicht
6.9	Wenn 6.9 nein: Nehmen Sie bitte umgehend mit dem AG Kontakt auf, um die Tätigkeit und Identität der bisher nicht genehmigten Subunternehmer zu klären.
6.10	Falls 6.8 ja: Wie stellen Sie sicher, dass Ihre Subunternehmer die Vorgaben dieses Vertrages mit dem AG und die Sie betreffenden Weisungen und Sicherheitsmaßnahmen umsetzen. Mehrfachantworten möglich!!! ☐ Kein Prozess hierzu vorhanden ☐ Die technisch-organisatorischen Sicherheitsmaßnahmen der Subunternehmer wurden bereits überprüft. Die Überprüfung wurde dokumentiert. Die Dokumentation wird dem AG auf Anfrage zur Verfügung gestellt. ☐ Die technisch-organisatorischen Sicherheitsmaßnahmen der Subunternehmer werden zeitnah überprüft. Die Überprüfung wird dokumentiert. Die Dokumentation wird dem AG anschließend zur Verfügung gestellt. x Mit den Subunternehmern werden Verträge nach EU DSGVO geschlossen. Diese können nach Aufforderung durch den AG vorgelegt werden. ☐ Eine Auftragskontrolle hat noch nicht stattgefunden.

+ 17

6.11	Wurde Ihr Unternehmen bereits einmal von einer Aufsichtsbehörde für den Datenschutz überprüft oder zertifiziert? ☐ ja x nein
6.12	Wenn 6.12 ja: Sind Sie in der Lage, die Dokumentation der Prüfung / Zertifizierung dem AG vorzulegen. ☐ ja ☐ nein

7. Verfügbarkeitskontrolle

A.	Serverseitig getroffene Verfügbarkeitskontrollmaßnahmen
7.1	Verfügt der Serverraum über eine feuerfeste / feuerhemmende Zugangstür (bspw. F 90)? x ja ☐ nein
7.2	Ist der Serverraum mit Rauchmeldern ausgestattet? x ja ☐ nein
7.3	Ist der Serverraum an eine Brandmeldezentrale angeschlossen? x ja ☐ nein
7.4	Ist der Serverraum mit Löschsystemen ausgestattet? Mehrfachantworten möglich! ☐ ja, CO2 Löscher x ja, Halon / Argon Löschanlage ☐ Sonstiges: bitte angeben
7.5	Woraus bestehen die Außenwände des Serverraumes? x Massivwand (bspw. Beton, Mauer) ☐ Leichtbauweise
7.6	Ist der Serverraum klimatisiert? x ja ☐ nein
7.7	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)? x ja ☐ nein
7.8	Wird deren Funktionalität regelmäßig getestet? x ja ☐ nein
7.9	Verfügt der Serverraum zusätzlich über ein Dieselaggregat? x ja ☐ nein
7.10	Existiert in Ihrem Unternehmen ein dokumentiertes Backup Konzept? x ja ☐ nein
7.11	Wird die Funktionalität der Backup Wiederherstellung regelmäßig getestet? x ja ☐ nein
7.12	Wenn 7.10 ja: Sind Sie in der Lage, dem AG auf Anforderung das Backup Konzept vorzulegen? x ja ☐ nein
7.13	In welchen Rhythmus werden in Ihrem Unternehmen Backups der Systeme angefertigt, auf denen die Auftragsdaten gespeichert werden? x Echtzeitspiegelung x täglich ☐ ein bis dreimal pro Woche ☐ Sonstiges: bitte angeben
7.14	Auf was für Sicherungsmedien werden die Backups gespeichert? x Zweiter redundanter Server ☐ Sicherungsbänder x Festplatten ☐ Sonstiges: bitte angeben

+ 18

7.15	Wo werden die Backups aufbewahrt / erstellt? x Zweiter redundanter Server steht an einem anderen Ort ☐ Safe, feuerfest, dokumentensicher ☐ einfacher Safe ☐ Bankschließfach ☐ abgeschlossener Aktenschrank / Schreibtisch x Im Serverraum ☐ Privathaushalt
7.16	Zu 7.15: Im Falle eines Transports der Backups: Wie wird dieser durchgeführt? ☐ Mitnahme durch einen MA der IT / Geschäftsleitung / Sekretärin ☐ Abholung durch Dritte (bspw. Bankmitarbeiter / Wachunternehmen) ☐ Sonstiges: bitte angeben
7.17	Sind die Daten der Sicherungen / Backups verschlüsselt? x ja ☐ nein
7.18	Befindet sich der Aufbewahrungsort nach Ziff. 7.15 in einem vom primären Server aus betrachtet getrennten Brandabschnitt / Gebäudeteil? x ja ☐ nein
B.	Allgemeine Verfügbarkeitskontrollmaßnahmen
7.19	Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisiertem x Virenschutz x Anti-Spyware x Spamfilter x Firewall
7.20	Existiert in Ihrem Unternehmen ein dokumentiertes Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)? x ja ☐ nein

+ 19

8. Trennungsgebot

8.1	Wie sind die Auftragsdaten des AG von anderen Daten (bspw. Daten des AN oder von anderen AG) getrennt? ☐ ja, logische Trennung ☐ ja, physische Trennung x nein
8.2	Sind die zur Verarbeitung der Auftragsdaten eingesetzten Verfahren mandantenfähig? ☐ ja ☐ nein x Es werden keine weiteren speziellen Verfahren eingesetzt, die Trennung erfolgt logisch auf Verzeichnisebene.

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

9.1	Werden die TOM's regelmäßig evaluiert? x ja ☐ nein
9.2	Wenn 9.1 ja: Wie oft erfolgt die Evaluation und durch wen? Die Evaluation erfolgt mindestens einmal pro Jahr und wird durch die IT und den Datenschutzbeauftragten durchgeführt.

Anhang 4 zum Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung:

Technisch-organisatorische Sicherheitsmaßnahmen **für Hosting**

1. Zutrittskontrolle

A.	Serverseitig getroffene Zutrittskontrollmaßnahmen
1.0	Werden die Auftragsdaten des Auftraggebers auf von Ihnen oder in Ihrem Auftrag betriebenen Servern physikalisch gespeichert? x ja ☐ nein
	Wenn 1.0 nein: In diesem Fall müssen Sie die Fragen 1.1 bis 1.29 nicht beantworten. Bitte gehen Sie dann gleich zu Frage 1.30 über! Auch die Fragen 7.1 bis 7.20 entfallen.
1.1	Nennen Sie bitte die genaue Adresse des Standorts des Serverraums / Rechenzentrums (RZ). Adresse des Serverstandortes: Nessus, Fernkorngasse 10, 1100 Wien
1.2	Sind die Auftragsdaten auf mehr als einen Serverstandort / Rechenzentrum verteilt (z. B. Backup Server/ Nutzung von Cloud-Dienstleistungen)? x ja ☐ nein
1.3	Falls 1.2 ja: Machen Sie bitte die entsprechenden Adressangaben auch bzgl. weiterer Server. Weitere Serverstandort: Nessus, Dampfgasse, 1100 Wien
1.4	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für alle im Einsatz befindlichen Server- / RZ Standorte? x ja ☐ nein
+ 20 1.5	Falls 1.4 nein: Beantworten Sie bitte die Fragen 1.6 bis 1.29 und 7.1 bis 7.20 für weitere RZ- / Serverstandorte.
1.6	Wird der Server / das RZ durch Sie (AN) selbst, oder durch einen Dienstleister / Subunternehmer betrieben? ☐ Auftragnehmer x Dienstleister
1.7	Sofern der Server durch einen Subunternehmer betrieben wird, nennen Sie bitte Namen und Sitz des Dienstleisters Digimagical GmbH, Legstattgasse 4-6/C25, 3001 Mauerbach, Österreich
1.8	Im wievielten Stock steht der Server, auf dem die Auftragsdaten gespeichert werden? ☐ EG ☐ Keller x 1. OG
1.9	Ist der Serverraum fensterlos? x ja ☐ nein
1.10	Wenn 1.9 nein: Wie sind die Fenster vor Einbruch geschützt? ☐ vergittert ☐ alarmgesichert ☐ abschließbar ☐ gar nicht ☐ Sonstiges: bitte eintragen
1.11	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? x ja ☐ nein
1.12	Wenn 1.11 ja: Wer wird informiert, wenn die EMA auslöst? Mehrfachantworten möglich! x beauftragter Wachdienst x Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
1.13	Ist der Serverraum mit einem elektronischen Schließsystem versehen? x ja ☐ nein
1.14	Wenn 1.13 ja: Welche Zutrittstechnik kommt zum Einsatz? Mehrfachantworten möglich! x RFID ☐ PIN x Biometrie ☐ Sonstiges: bitte eintragen

1.15	Wenn 1.13 ja: Sind die Zutrittstechniken personenbezogen vergeben / personifiziert? x ja ☐ nein
1.16	Wenn 1.13 ja: Werden die Zutritte zum Raum im Zutrittssystem gespeichert/protokolliert? x ja, sowohl erfolgreiche / positive, als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche / positive Zutritte ☐ nein, das Schloss wird nur freigegeben oder nicht
1.17	Wenn 1.16 ja: Wie lange werden die Zutrittsdaten ungefähr gespeichert? 30 Tage
1.18	Existiert ein mechanisches Schloss? ☐ ja x nein
1.19	Wenn 1.18 ja, wie viele Schlüssel zum Serverraum existieren und wo werden diese aufbewahrt. Anzahl Schlüssel: Aufbewahrungsort:
1.20	Wenn 1.18 ja: Wird die Schlüsselausgabe protokolliert? ☐ ja ☐ nein
1.21	Wenn 1.18 ja: Wie wird protokolliert und wer gibt die Schlüssel aus? ☐ Schlüsselbuch Ausgabestelle: bitte Ausgabestelle angeben
1.22	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Siehe Anhang 2 (Ansprechpartner Digimagical)
1.23	Ist der Serverraum videoüberwacht? x ja ☐ nein
1.24	Wenn 1.23 ja: Wie lange werden die Bilddaten gespeichert? 30 Tage
1.25	Wie ist der Zutritt durch betriebsfremde Personen zum Serverraum geregelt? (bspw. Im Falle von Wartungsdiensten / Elektrikern / Reinigungspersonal). ☐ es gibt keine Regelung x Zutritt & Anwesenheit nur in Begleitung ☐ Sonstiges: bitte eintragen
1.26	Werden Zutritte durch Betriebsfremde zum Serverraum protokolliert? x ja ☐ nein
1.27	Aus welchem Material besteht die Zugangstür zum Serverraum? x Stahl / Metall ☐ sonstiges Material
1.28	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt? ☐ ja x nein
1.29	Wenn 1.28 ja: Was wird in dem Serverraum noch aufbewahrt? ☐ Telefonanlage ☐ Lagerung Büromaterial ☐ Lagerung Akten ☐ Archiv ☐ Lagerung von IT Ausstattung ☐ Sonstiges: bitte eintragen

+ 21

B.	Clientseitig getroffene Zutrittskontrollmaßnahmen
1.30	Nennen Sie bitte die genaue Adresse des Standorts der Clientarbeitsplätze, von denen auf die Auftragsdaten zugegriffen wird. Troi GmbH, Gabrielenstraße 9, 80636 München, Deutschland (Details siehe Anhang 3) Digimagical GmbH, Fernkorngasse 10/Stiege 3/DG in 1100 Wien, Österreich

1.31	Ist das Bürogebäude vollständig umfriedet (Zaun, Mauer o.ä.). x ja ☐ nein
1.32	Im wievielten Stock befinden sich die Büroräume? ☐ EG ☐ Keller ☐ im gesamten Gebäude x Nur im 5. OG
1.33	Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros? ☐ ja x nein
1.34	Wird ein Besucherbuch geführt? ☐ ja x nein
1.35	Ist das Gebäude / die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? x ja ☐ nein
1.36	Wenn 1.35 ja: Wer wird informiert, wenn die EMA auslöst? x beauftragter Wachdienst x Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
1.37	Ist das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen? ☐ ja, Gebäude und Büroräume sind elektronisch verschlossen ☐ ja, aber nur das Gebäude, nicht der Eingang zu den Büros / zur Büroetage. x ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt. ☐ nein
1.38	Wenn ja 1.37: Welche Zutrittstechnik kommt zum Einsatz? Mehrfachantworten möglich! ☐ RFID ☐ PIN x Biometrie ☐ Sonstiges: bitte eintragen
1.39	Wenn 1.37 ja: Sind die Zutrittstechniken personenbezogen vergeben / personifiziert? x ja ☐ nein
1.40 **+ 22**	Wenn 1.37 ja: Werden die Zutritte im Zutrittssystem gespeichert/protokolliert? x ja, sowohl erfolgreiche / positive, als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche / positive Zutritte ☐ nein, das Schloss wird nur freigegeben oder nicht.
1.41	Wenn 1.40 ja: Wie lange werden die Zutrittsdaten ungefähr gespeichert? 30 Tage
1.42	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? x ja ☐ nein
1.43	Wird die Ausgabe von Schlüsseln protokolliert und wer gibt die Schlüssel aus? ☐ nein, die Ausgabe wird nicht protokolliert x ja, die Ausgabe wird mittels eines Formulars / Schlüsselbuch dokumentiert. Ausgabestelle ist: Digimagical GmbH
1.44	Ist das Bürogebäude, bzw. seine Zugänge videoüberwacht? ☐ ja, ohne Bildaufzeichnung x ja, mit Bildaufzeichnung ☐ nein
1.45	Wenn 1.44 „ja, mit Bildaufzeichnung“, wie lange werden die Bilddaten gespeichert? 30 Tage

C.	Generelle Maßnahmen

1.46	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher; Fremdpersonal) zu den Büroräumen? ☐ nein x ja, betriebsfremde Personen werden am Eingang / Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.

2. Zugangskontrolle

2.1	Existiert ein persönlicher Passwort / (PW) Benutzername Zugangsschutz zu den Systemen, mit denen die Auftragsdaten verarbeitet werden? x ja ☐ nein
2.2	Wie werden die Zugangsberechtigungen vergeben? x auf Antrag (schriftlich oder Mail) an IT ☐ Antrag muss durch Vorgesetzten genehmigt sein ☐ Sonstige Vergabeweise: bitte angeben
2.3	Existiert für die Administration der Systeme ein eigenständiger ADMIN-Account, der sich von seinem eigentlichen User-Account des Admins unterscheidet? x ja ☐ nein, der Admin benutzt die Systeme immer als angemeldeter ADMIN
2.4	Existieren verbindliche Passwortparameter im Unternehmen? x ja ☐ nein
2.5	Wie lauten die Passwort (PW) Vorgaben: PW Länge: x 8 Zeichen oder mehr ☐ Weniger als 8 Zeichen ☐ Weniger als 6 Zeichen Welche Zeichenarten müssen erfüllt sein? x Sonderzeichen ☐ Ziffern ☐ Groß- / Kleinschreibung Gültigkeitsdauer des PW: ☐ 90 Tage oder weniger x 180 Tage oder weniger ☐ mehr als 180 Tage
2.6	Nach wie vielen Zyklen darf ein Nutzer dasselbe PW frühestens erneut vergeben (Passworthistorie)? ☐ keine Vorgabe ☐ 1 - 2 Zyklen ☐ 3 – 5 Zyklen x mehr als 5 Zyklen
2.7	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben? x ja ☐ nein
2.8	Ist eine automatische PW geschützte Bildschirmsperre eingestellt? x ja ☐ nein
2.9	Wenn 2.8 ja, Nach wie vielen Minuten der Inaktivität aktiviert sich die Bildschirmsperre? 5 Minuten
2.10	Existieren verbindliche Vorgaben zum manuellen Sperren des Clients beim Verlassen des Arbeitsplatzes? x ja, der Rechner ist manuell zu sperren ☐ nein
2.11	Kontrollieren Sie die Aktualität der Zugangsberechtigungen? x ja, regelmäßig ☐ nein, nur im Falle eines konkreten Anlasses
2.12	Welche Maßnahmen ergreifen Sie bei Verlust / Vergessen / Ausspähen eines PW? x Admin setzt neues PW, das der Nutzer dann nach Erstanmeldung zu ändern hat ☐ keine

+ 23

2.13	Gibt es eine Begrenzung von Anmeldeversuchen mit einem Benutzernamen / PW? x ja ☐ nein
2.14	Wenn 2.13 ja, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre durch die IT gesperrt x Die Zugänge bleiben für 30 Minuten gesperrt.
2.15	Bei Fernzugängen (VPN / IPSec): Mehrfachantworten möglich! Authentisierung mit x pre-shared key ☐ Zertifikat PW Länge: x 8 Zeichen oder mehr ☐ Weniger als 8 Zeichen ☐ Weniger als 6 Zeichen Welche Zeichenarten müssen erfüllt sein? x Sonderzeichen ☐ Ziffern ☐ Groß- / Kleinschreibung Gültigkeitsdauer des PW: ☐ 90 Tage oder weniger x 180 Tage oder weniger ☐ mehr als 180 Tage
2.16	Gibt es eine Begrenzung von Anmeldeversuchen bei Fernzugängen? x ja ☐ nein
2.17	Wenn 2.16 ja, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre durch die IT gesperrt x Die Zugänge bleiben für 30 Minuten gesperrt.
2.18	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? x ja ☐ nein
2.19 **+ 24**	Wie viele MA haben über Fernzugänge Zugang auf die Daten des AG? 5 Personen. Läuft der Zugang über die Fernzugänge über ☐ Sammelkennung x individuelle Einzelkennung
2.20	Werden die Systeme, auf denen die Daten des Auftraggebers verarbeitet werden, über eine Firewall abgesichert? x ja ☐ nein
2.21	Wenn 2.20 ja: Wird die Firewall regelmäßig upgedatet? x ja ☐ nein
2.22	Wenn 2.20 ja: Wer administriert Ihre Firewall? x eigene IT ☐ Externer Dienstleister
2.23	Wenn ein externer DL zum Einsatz kommt: Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten? ☐ ja ☐ nein, die Aufschaltung ist nur im 4 Augenprinzip mit einem Mitarbeiter der eigenen IT möglich.
2.24	Wenn ein externer DL zum Einsatz kommt: Haben Sie einen Vertrag zur Auftragsdatenverarbeitung mit diesem abgeschlossen? ☐ ja ☐ nein

3. Zugriffskontrolle

3.1	Existiert ein differenzierendes Berechtigungskonzept, das den Zugriff Ihrer Mitarbeiter auf die Daten des Auftraggebers regelt? x ja ☐ nein
3.2	Wie werden die Zugriffsberechtigungen Ihrer Mitarbeiter auf die Daten des Auftraggebers vergeben? Mehrfachantworten möglich! x auf Antrag (schriftlich oder Mail) an IT x Antrag muss durch Vorgesetzten genehmigt sein
3.3	Wie wird gewährleistet, dass die Zugriffsberechtigungen bei Abteilungs- / Funktionswechsel und / oder Ausscheiden eines Mitarbeiters aktualisiert / entzogen werden? Mehrfachantworten möglich! x personelle Veränderungen werden der IT Abteilung durch die Personalabteilung gemeldet. ☐ die zuständigen Vorgesetzten haben personelle Änderungen in ihrer Abteilung an die IT zu melden. ☐ Die Berechtigungen werden nach Art der Änderungen / des Wechsels angepasst bzw. entzogen. ☐ Sonstiges: bitte angeben
3.4	Werden Vergabe / Änderungen von Zugriffsberechtigungen protokolliert? x ja ☐ nein
3.5	Existieren getrennte Produktiv- und Testsysteme im Falle der Notwendigkeit der Wartung der Systeme? x ja ☐ nein
3.6	Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten, CD-ROMs, DVDs / Disketten), auf denen Auftragsdaten gespeichert sind, in Ihrem Unternehmen entsorgt? x Physikalische Zerstörung durch eigene IT. ☐ Physikalische Zerstörung durch externen Dienstleister. ☐ Sonstiges: bitte angeben
3.7	Wie werden nicht mehr benötigte Unterlagen mit personenbezogenen Daten des Auftraggebers (bspw. Ausdrucke / Akten / Schriftwechsel) in Ihrem Unternehmen entsorgt? ☐ Altpapier / Restmüll x Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist. ☐ Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden. x Sonstiges: Der verwendete Schredder entspricht der Sicherheitsstufe 4.
3.8	Wenn bei Ziff. 3.7 ein externer DL zum Einsatz kommt: Haben Sie einen Vertrag zur Auftragsdatenverarbeitung mit diesem abgeschlossen? ☐ ja ☐ nein
3.9	Dürfen Ihre MA eigene Speichermedien (z.B. USB Sticks) verwenden? ☐ generell ja ☐ ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT. x nein, alle benötigten Speichermedien werden vom Unternehmen gestellt.

+ 25

4. Weitergabekontrolle

4.1	Wie erfolgt der Datentransfer zwischen Ihnen und dem AG? Mehrfachantworten sind möglich! x Webportal ☐ mobiler Datenträger x E-Mail (Text und Anhänge wie PDF- / Excel- / Worddateien) ☐ Fax ☐ Schriftlich x telefonisch x FTP Server ☐ Share Point

	☐ Einsichtnahme am Monitor (bspw. Fernwartung per Teamviewer o.ä.) ☐ Sonstiges (z.B. Clouddienste wie Drop Box): bitte angeben
4.2	Wenn die Daten elektronisch übertragen werden, erfolgt dieser Transfer verschlüsselt / technisch geschützt? ☐ nein (z.B. http / FTP) ☐ nein, aber persönliche Übergabe (bspw. Ausdrucke, Speichermedien wie bspw. DVDs) x ja, per PW geschütztem ZIP Archiv / PDF / Excel File als Mailanhang ☐ ja, per PGP ☐ ja, per verschlüsselten Datenträger ☐ ja, per verschlüsseltem VPN x ja, per https / SSL x ja, per SFTP ☐ ja, Sonstiges: bitte angeben
4.3	Gibt es eine Vereinbarung, welche Personen auf Seite des AG und des AN die Daten übertragen dürfen? x ja ☐ nein
4.4	Wenn 4.3 ja: Wer ist jeweils zur Übertragung von Auftragsdaten befugt? Siehe Anhang 2
4.5	Werden die Übertragungsvorgänge protokolliert? x ja ☐ nein
4.6	Werden Auftragsdaten des AG durch Ihr Unternehmen (bzw. Ihre Mitarbeiter) auch auf mobilen Endgeräten verarbeitet? x ja ☐ nein
4.7	Wenn 4.6 ja: Wie sind die Endgeräte bzw. die darauf gespeicherten Auftragsdaten bei der Übertragung gesichert? Mehrfachantworten sind möglich! ☐ außer dem Schutz durch die allgemeine PW / Benutzerkennung keine weiteren Maßnahmen. x Verschlüsselung der Festplatten / Verzeichnisse gem. modernen Standards x über eine VPN-Verbindung zum eigenen Firmennetz x über eine VPN-Verbindung zum Auftraggeber ☐ Sonstiges: bitte angeben
4.8	Wenn 4.6 ja: Verarbeiten Ihre Mitarbeiter Auftragsdaten des AG auch auf eigenen privaten Geräten (bring your own device)? ☐ ja x nein
4.9	Können Ihre Mitarbeiter auf die Daten des Auftraggebers vom Home-Office aus zugreifen. x ja ☐ nein x Sonstiges: Für Arbeiten im Home-Office oder von unterwegs werden ausschließlich dienstliche Endgeräte genutzt. Verbindungen in das Rechenzentrum werden ausschließlich über VPN ermöglicht. Der Einsatz privater Geräte ist verboten.

+ 26

5. Eingabekontrolle

5.1	Werden Zugriffe (Lesen, Änderungen, Löschen) auf Daten des Auftraggebers personenbezogen protokolliert? x ja ☐ nein
5.2	Wenn 5.1 ja: Wie lange werden diese Protokolldaten aufbewahrt? 180 Tage
5.3	Wenn 5.1 ja: Werden die Protokolle ausgewertet? x ja ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich
5.4	Wenn 5.1 nein: Ist zumindest der letzte Zugriff auf die Daten (Uhrzeit / Datum der Änderung) feststellbar? ☐ ja ☐ nein

6. Auftragskontrolle

6.1	Hat Ihr Unternehmen schriftlich einen fachkundigen Datenschutzbeauftragten (DSB) bestellt? ☐ ja, interner DSB (Mitarbeiter des Auftragnehmers) x ja, externer DSB ☐ nein
6.2	Wenn 6.1 ja: Nennen Sie bitten den Namen und Kontaktdaten Ihres DSB. IITR Datenschutz GmbH Dr. Sebastian Kraska Marienplatz 2 80331 München E-Mail: email@iitr.de Telefon: +49 (089) 18917360 Impressum: https://www.iitr.de/unternehmen/impressum.html
6.3	Wenn 6.1 ja: Welche nachweisbare Qualifikation besitzt der bestellte DSB? ☐ keine ☐ nachweisbare Lehrgangsteilnahme zum Datenschutzbeauftragten (bspw. beim TÜV, IHK o.ä.) x es handelt sich um einen Juristen ☐ es handelt sich um einen Informatiker ☐ Sonstige Qualifikation: bitte angeben
6.4	Werden Ihre MA, die Auftragsdaten verarbeiten, nachweislich im Datenschutzrecht geschult? ☐ ja, Präsenzschulungen ☐ ja, eLearning x Merkblätter / Handouts ☐ nein
6.5	Werden Ihre MA schriftlich auf das Datengeheimnis verpflichtet? x ja ☐ nein
6.6	Werden Ihre MA (soweit erforderlich) schriftlich auf das Sozialgeheimnis verpflichtet? ☐ ja x nein
6.7	Setzen Sie zur Erfüllung Ihrer Pflichten aus dem Vertrag mit dem AG auch weitere Subunternehmer ein? x ja ☐ nein
6.8	Sind die von Ihnen eingesetzten Subunternehmer dem AG gegenüber benannt worden und vom AG genehmigt? x ja siehe Anhang 2 ☐ nein, bisher noch nicht
6.9	Wenn 6.9 nein: Nehmen Sie bitte umgehend mit dem AG Kontakt auf, um die Tätigkeit und Identität der bisher nicht genehmigten Subunternehmer zu klären.
6.10	Falls 6.8 ja: Wie stellen Sie sicher, dass Ihre Subunternehmer die Vorgaben dieses Vertrages mit dem AG und die Sie betreffenden Weisungen und Sicherheitsmaßnahmen umsetzen. Mehrfachantworten möglich!!! ☐ Kein Prozess hierzu vorhanden ☐ Die technisch-organisatorischen Sicherheitsmaßnahmen der Subunternehmer wurden bereits überprüft. Die Überprüfung wurde dokumentiert. Die Dokumentation wird dem AG auf Anfrage zur Verfügung gestellt. ☐ Die technisch-organisatorischen Sicherheitsmaßnahmen der Subunternehmer werden zeitnah überprüft. Die Überprüfung wird dokumentiert. Die Dokumentation wird dem AG anschließend zur Verfügung gestellt. x Mit den Subunternehmern werden Verträge nach EU DSGVO geschlossen. Diese können nach Aufforderung durch den AG vorgelegt werden. ☐ Eine Auftragskontrolle hat noch nicht stattgefunden.

+ 27

6.11	Wurde Ihr Unternehmen bereits einmal von einer Aufsichtsbehörde für den Datenschutz überprüft oder zertifiziert? ☐ ja x nein
6.12	Wenn 6.12 ja: Sind Sie in der Lage, die Dokumentation der Prüfung / Zertifizierung dem AG vorzulegen. ☐ ja ☐ nein

7. Verfügbarkeitskontrolle

A.	Serverseitig getroffene Verfügbarkeitskontrollmaßnahmen
7.1	Verfügt der Serverraum über eine feuerfeste / feuerhemmende Zugangstür (bspw. F 90)? x ja ☐ nein
7.2	Ist der Serverraum mit Rauchmeldern ausgestattet? x ja ☐ nein
7.3	Ist der Serverraum an eine Brandmeldezentrale angeschlossen? x ja ☐ nein
7.4	Ist der Serverraum mit Löschsystemen ausgestattet? Mehrfachantworten möglich! ☐ ja, CO2 Löscher x ja, Halon / Argon Löschanlage ☐ Sonstiges: bitte angeben
7.5	Woraus bestehen die Außenwände des Serverraumes? x Massivwand (bspw. Beton, Mauer) ☐ Leichtbauweise
7.6	Ist der Serverraum klimatisiert? x ja ☐ nein
+ 28 7.7	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)? x ja ☐ nein
7.8	Wird deren Funktionalität regelmäßig getestet? x ja ☐ nein
7.9	Verfügt der Serverraum zusätzlich über ein Dieselaggregat? x ja ☐ nein
7.10	Existiert in Ihrem Unternehmen ein dokumentiertes Backup Konzept? x ja ☐ nein
7.11	Wird die Funktionalität der Backup Wiederherstellung regelmäßig getestet? x ja ☐ nein
7.12	Wenn 7.10 ja: Sind Sie in der Lage, dem AG auf Anforderung das Backup Konzept vorzulegen? x ja ☐ nein
7.13	In welchen Rhythmus werden in Ihrem Unternehmen Backups der Systeme angefertigt, auf denen die Auftragsdaten gespeichert werden? x Echtzeitspiegelung x täglich ☐ ein bis dreimal pro Woche ☐ Sonstiges: bitte angeben
7.14	Auf was für Sicherungsmedien werden die Backups gespeichert? x Zweiter redundanter Server ☐ Sicherungsbänder x Festplatten ☐ Sonstiges: bitte angeben

7.15	Wo werden die Backups aufbewahrt / erstellt? x Zweiter redundanter Server steht an einem anderen Ort ☐ Safe, feuerfest, dokumentensicher ☐ einfacher Safe ☐ Bankschließfach ☐ abgeschlossener Aktenschrank / Schreibtisch x Im Serverraum ☐ Privathaushalt
7.16	Zu 7.15: Im Falle eines Transports der Backups: Wie wird dieser durchgeführt? ☐ Mitnahme durch einen MA der IT / Geschäftsleitung / Sekretärin ☐ Abholung durch Dritte (bspw. Bankmitarbeiter / Wachunternehmen) ☐ Sonstiges: bitte angeben
7.17	Sind die Daten der Sicherungen / Backups verschlüsselt? x ja ☐ nein
7.18	Befindet sich der Aufbewahrungsort nach Ziff. 7.15 in einem vom primären Server aus betrachtet getrennten Brandabschnitt / Gebäudeteil? x ja ☐ nein
B.	Allgemeine Verfügbarkeitskontrollmaßnahmen
7.19	Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisiertem x Virenschutz x Anti-Spyware x Spamfilter x Firewall
7.20	Existiert in Ihrem Unternehmen ein dokumentiertes Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)? x ja ☐ nein

8. Trennungsgebot

+ 29

8.1	Wie sind die Auftragsdaten des AG von anderen Daten (bspw. Daten des AN oder von anderen AG) getrennt? ☐ ja, logische Trennung x ja, physische Trennung ☐ nein
8.2	Sind die zur Verarbeitung der Auftragsdaten eingesetzten Verfahren mandantenfähig? x ja ☐ nein ☐ Es werden keine weiteren speziellen Verfahren eingesetzt, die Trennung erfolgt logisch auf Verzeichnisebene.

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

9.1	Werden die TOM's regelmäßig evaluiert? x ja ☐ nein
9.2	Wenn 9.1 ja: Wie oft erfolgt die Evaluation und durch wen? Die Evaluation erfolgt mindestens einmal pro Jahr und wird durch die IT und den Datenschutzbeauftragten durchgeführt.