Zusatzvereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

Name: _____

Straße: _____

PLZ/Ort: _____

Land: _____

- Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO, nachstehend **Auftraggeber** genannt -

und

OpenProject GmbH

Karl-Liebknecht-Str. 5

10178 Berlin

Deutschland

- Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DS-GVO, nachstehend **Auftragnehmer** genannt -

Präambel

Diese Vereinbarung zur Auftragsverarbeitung regelt die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Leistungsvertrag nebst Produktbeschreibungen ergeben.

Produkt: OpenProject Cloud Edition

Kundennummer: _____

Vertragsnummer (URL): _____

Abschlussdatum: _____

Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Der Auftragnehmer wird für den Auftraggeber personenbezogene Daten ausschließlich im Rahmen dieser Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO erheben, verarbeiten und sonst wie nutzen.

§ 1 Anwendungsbereich und Verantwortlichkeit

(1) Der Gegenstand, Art und Zweck des Auftrags sind Tätigkeiten, deren Konkretisierung sich aus dem oben bezeichneten Leistungsvertrag und den zugehörigen Produktbeschreibungen ergeben.

(2) Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien und/oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Der Auftraggeber ist alleine verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchgeführten Erhebungen, Verarbeitungen und Nutzungen personenbezogener Daten durch den Auftragnehmer im Hinblick auf die Regelungen der Europäischen Datenschutzgrundverordnung (DS-GVO) und anderer einschlägiger Vorschriften über den Datenschutz.

§ 2 Ort der vorgesehenen Verarbeitung von Daten

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Die Übermittlung personenbezogener Daten an Stellen, die weder in einem Mitgliedsstaat der Europäi-

schen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum ansässig sind (sog. Drittstaat), bedarf der Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 3 Art der Daten und Kreis der Betroffenen

(1) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- Vor- und Zuname
- E-Mail-Adresse
- Unternehmensname
- Telefonnummer
- Rechnungsadresse
- Bankverbindung
- Umsatzsteuer-Identifikationsnummer
- Profilbild (Avatar-Bild)

(2) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers
- Lieferanten des Auftraggebers

§ 4 Technisch-organisatorische Maßnahmen

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Die vom Auftragnehmer ergriffenen Maßnahmen sind in Anlage 1 dieser Vereinbarung zur Auftragsverarbeitung aufgeführt. Der Auftragnehmer wird die Dokumentation der technischen und organisatorischen Maßnahmen auf dem jeweils aktuellen Stand halten.

§ 5 Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer wird die Daten, die im Auftrag verarbeitet werden, nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.

§ 6 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für alle Daten, automatisierte Verfahren und Datenverarbeitungsanlagen in seinem Zuständigkeitsbereich sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich.

(2) Der Auftraggeber hat die technischen und organisatorischen Maßnahmen zu veranlassen, die erforderlich sind, um den Datenschutz und die Datensicherheit bei der Auftragsabwicklung zu gewährleisten. Art und Umfang der Arbeiten sowie die Befugnisse des eingesetzten Personals des Auftragnehmers sind hinreichend festzulegen. Die Kosten solcher technischen und organisatorischen Maßnahmen, die aufgrund einer besonderen Anforderung des Auftraggebers im Betrieb des Auftragnehmers implementiert werden müssen, trägt der Auftraggeber.

(3) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf der Arbeiten zu erteilen; sie sind schriftlich zu fassen. Mündliche Weisungen hat der Auftraggeber unverzüglich schriftlich zu bestätigen.

(4) Die weisungs-, empfangs- und kontrollberechtigten Personen sind schriftlich zu benennen. Sie haben sich bei der Ausübung ihrer Befugnisse zu legitimieren.

§ 7 Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieser Vereinbarung die gesetzlichen Pflichten gemäß Art. 28 bis 33 DS-GVO zu erfüllen; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind in Anlage 1 aufgeführt.

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten des Auftraggebers haben, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in dieser Vereinbarung zur Auftragsverarbeitung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO. Die technischen und organisatorischen Maßnahmen sind in Anlage 1 zu dieser Vereinbarung dokumentiert.

(4) Die Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf das zugrundeliegende Auftragsverhältnis beziehen.

(5) Auskünfte gegenüber betroffenen Personen oder Dritten, das zugrundeliegende Auftragsverhältnis betreffend, darf der Auftragnehmer nur mit Zustimmung des Auftraggebers erteilen, es sei denn er ist gesetzlich dazu verpflichtet.

§ 8 Unterauftragnehmer

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer mit der Verarbeitung personenbezogener Daten des Auftraggebers nur beauftragen, soweit diese in einem Mitgliedsstaat der Europäischen Union (EU) oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) ansässig sind. Die Weiterleitung, Speicherung und Datenverarbeitung auf automatisierten Datenverarbeitungsanlagen außerhalb der EU oder des EWR ist nicht zulässig.

(3) Der Auftraggeber stimmt der Beauftragung der vom Auftragnehmer in Anlage 2 dieser Vereinbarung genannten Unterauftragnehmer, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO, zu.

(4) Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel eines bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber vor Beginn der Verarbeitung durch den Unterauftragnehmer schriftlich oder in Textform anzeigt. Das Widerspruchsrecht des Auftraggebers gilt zwei Wochen ab Anzeige und erfolgt ebenfalls schriftlich oder in Textform.
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(5) Der Auftragnehmer wird die Einhaltung der datenschutzrechtlichen Anforderungen beim Unterauftragnehmer regelmäßig überprüfen.

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

§ 9 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, nach angemessener Vorankündigung, Überprüfungen durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer wird dem Auftraggeber nach vorheriger Terminvereinbarung Zugang zu Grundstücken und Geschäftsräumen des Auftragnehmers während der vor Ort üblichen Betriebs- und Geschäftszeiten gewähren. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(2) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO; die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz).

§ 10 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten, Störungen, Verstöße des Auftragnehmers oder der bei ihm Beschäftigten oder von ihm beauftragten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen, mit. Dies gilt vor allem auch im Hinblick auf eventuelle gesetzliche Informationspflichten des Auftraggebers gegenüber betroffenen Personen oder Aufsichtsbehörden.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 30 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen nach Möglichkeit. Hierzu gehören insbesondere:

- Untergliederung der Einrichtung in einzelne Sicherheitsbereiche,
- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
- die Verpflichtung, Verletzungen personenbezogener Daten an den Auftraggeber zu melden;
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen zu unterstützen;

- die Unterstützung des Auftraggebers bei dessen Pflichten zur Durchführung von Datenschutz-Folgenabschätzungen;
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 11 Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 12 Dauer des Auftrags

(1) Die Gültigkeit dieser Vereinbarung zur Auftragsverarbeitung (Laufzeit) entspricht der Laufzeit des Leistungsvertrages gemäß § 1. Die Geheimhaltungspflicht reicht über das Vertragsende hinaus.

(2) Die Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen durch den Auftragnehmer ist ein wichtiger Grund für den Auftraggeber, das in den vertraglichen Vereinbarungen des unter § 1 genannten Leistungsvertrages vorbehaltene Recht zur außerordentlichen Kündigung auszuüben.

§ 13 Salvatorische Klausel

Sollten einzelne oder mehrere Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, so wird hierdurch die Gültigkeit der übrigen Regelungen dieser Vereinbarung nicht berührt.

§ 14 Schlussbestimmungen

(1) Änderungen oder Ergänzungen zu dieser Vereinbarung bedürfen der Schriftform und sind von beiden Vertragsparteien zu unterschreiben. Dies gilt auch für die Änderung dieser Schriftformklausel. E-Mail wahrt die Schriftform nicht.

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

(3) Es gilt ausschließlich das Recht der Bundesrepublik Deutschland. Gerichtsstand für alle Streitigkeiten aus diesem oder im Zusammenhang mit diesem Vertrag ist Berlin.

§ 15 Inkrafttreten

Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft.

§ 16 Anhänge

Dieser Vereinbarung zur Auftragsverarbeitung sind folgende Anlagen beigefügt:

- Anlage 1: Technisch-organisatorische Maßnahmen
- Anlage 2: Liste der eingesetzten Unterauftragnehmer

§ 17 Unterschriften

_____, den _____ _____, den _____

Ort Datum Ort Datum

_____ _____

- Auftraggeber - - Auftragnehmer (OpenProject GmbH) –

Anlage 1: Technische und organisatorische Maßnahmen zur Datensicherheit

Die in dieser Anlage durch den Auftragnehmer definierten Datensicherheitsmaßnahmen werden als verbindlich festgelegt.

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

1.1. Zutrittskontrolle

Die Datenverarbeitung durch den Auftragnehmer findet in einem gesicherten Rechenzentrum statt. Das Rechenzentrum ist nach Standard ISO 27001 für das Informationssicherheits-Managementsystem zertifiziert. Der Zutritt zu dem Rechenzentrum wird durch modernste Kontrollsysteme gesichert. Hierzu gehören folgende Sicherheitsmaßnahmen und -infrastrukturen:

- Untergliederung der Einrichtung in einzelne Sicherheitsbereiche,
- physikalischer Zutrittsschutz beispielsweise durch Stahltüren, fensterlose Räume oder gesicherte Fenster,
- Schutz der Sicherheitsbereiche durch ein elektronisches Zutrittskontrollsystem,
- Überwachung der Einrichtung durch Sicherheitsdienst und Protokollierung der Zutritte,
- Videoüberwachung aller sicherheitsrelevanten Sicherheitsbereiche, wie Eingänge, Notausgänge und Serverräume,
- zentrale Vergabe und Entzug der Zutrittsberechtigung,
- Identifikation aller Besucher mittels Personalausweis,
- Ausweispflicht innerhalb der Sicherheitsbereiche für alle Mitarbeiter und Besucher,
- kontinuierliche Begleitung von Besuchern durch Mitarbeiter.

1.2. Zugangskontrolle

Der Auftragnehmer hat das Eindringen Unbefugter in Systeme und Anwendungen, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden, zu verhindern. Der Auftragnehmer gewährleistet dies, indem ausschließlich explizit autorisierte Administratoren Zugang zu den datenverarbeitenden Systemen des IaaS-Anbieters erhalten. Die Anmeldung erfolgt ausschließlich per Multi-Faktor-Authentifizierung anhand der im jeweiligen persönlichen Benutzerkonto hinterlegten Anmelde-Informationen. Darüber hinaus kommt ein differenziertes Rechtesystem anhand von Sicherheitsgruppen und Zugriffskontrolllisten zum Einsatz. Die Anmeldung ist ausschließlich über Verbindungen möglich, welche über den aktuellen Stand der Technik verschlüsselt werden.

Zu weiteren Absicherung des Zugangs sind die einzelnen Dienste und Komponenten in mehrere Netzwerksegmente aufgeteilt. Die Isolation erfolgt durch hardwarebasierte Firewall-Systeme und Virtual Private Clouds (VPC). Sämtliche Zugänge auf Systeme und Anwendungen werden zentral dokumentiert, überwacht und protokolliert.

Das bürointerne Netzwerk wird durch eine hardwarebasierte Firewall gegen den unbefugten Zugang von außen geschützt. Der Zugang zu Rechnern in den Büroräumen des Auftragnehmers wird über Benutzerkonten kontrolliert. Auf das bürointerne Netzwerk kann von außerhalb der Büroräume ausschließlich über eine verschlüsselte VPN-Verbindung (Virtual Private Network) zugriffen werden.

Der Auftraggeber kann auf seine OpenProject-Instanz ausschließlich über eine verschlüsselte Verbindung (SSL/HTTPS) zugreifen.

1.3. Zugriffskontrolle

Der Auftragnehmer hat unerlaubte Tätigkeiten in den datenverarbeitenden Systemen zu verhindern. Demzufolge hat ausschließlich der betreffende Auftraggeber sowie eine kleine Gruppe einzeln benannter Administratoren Zugriff auf die Daten. Es wird technisch sichergestellt, dass ein Auftraggeber keine Daten anderer Auftraggeber einsehen, verändern oder löschen kann. Innerhalb einer OpenProject-Instanz wird der Zugriff über ein umfangreiches Rollen- und Berechtigungskonzept gesteuert. Innerhalb der OpenProject Instanz erfolgt die Rechtevergabe durch den Auftraggeber durch Rollen- und Rechtezuweisungen. Der Auftraggeber hat zusätzlich die Möglichkeit, für seine Organisation über eine Administrationsoberfläche die vorkonfigurierten Rollen und Rechte auf seine Bedürfnisse hin anzupassen.

Der Zugriff auf Daten des Auftraggebers für Kundendienst-Mitarbeiter des Auftragnehmers ist auf Stammdaten und Abrechnungsdaten beschränkt, welche für die Wahrnehmung ihrer Kundendienst-Aufgabe und der Abrechnung der Hosting-Dienstleistung erforderlich sind. Kundendienst-Mitarbeiter haben keinen Zugriff auf die Kundendaten innerhalb einer OpenProject-Instanz.

Kreditkarten-Daten ihrer Auftraggeber werden ausschließlich durch den Bezahldienstleister gespeichert; der Auftragnehmer hat keinen Zugriff auf diese Daten.

Administratoren ist der Zugriff auf Kundendaten nur gestattet, wenn eine Störung vorliegt, die nicht durch den Auftraggeber und oder den Kundendienst des Auftragnehmers alleine gelöst werden kann.

1.4. Trennungskontrolle

Sämtliche Datensätze, die von den Systemen und Anwendungen des Auftragnehmers erhoben, verarbeitet oder genutzt werden, werden explizit und eindeutig dem jeweiligen Auftraggeber zugeordnet und technisch von anderen Daten getrennt. Die datenverarbeitenden Systeme des Auftragnehmers sind speziell auf die zweckgebundene und mandantengerechte Verarbeitung ausgerichtet. Der Zugriff auf die Daten eines anderen Auftraggebers ist damit technisch ausgeschlossen.

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Pseudonymisierung soll gewährleisten, dass die Identifizierung der von der Datenverarbeitung betroffenen Person ausgeschlossen bzw. wesentlich erschwert wird.

Die Daten von gelöschten Nutzern in OpenProject werden annonymisiert, sodass keine Zuordnung zu den jeweiligen Personen mehr möglich ist.

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

2.1. Weitergabekontrolle

Die Kontrolle der Weitergabe von Daten des Auftraggebers wird durch verschiedene technische und organisatorische Sicherheitsmaßnahmen gewährleistet. Hierbei verarbeitet oder speichert der Auftragnehmer Daten des Auftragnehmers grundsätzlich nicht außerhalb des Rechenzentrums. Mitarbeiter des Rechenzentrumbetreibers haben keinen Zugriff oder Zugang zu den Kundendaten, können diese also weder einsehen, löschen oder verändern. Datensicherungen werden ausschließlich verschlüsselt abgelegt. Ein Transport von Daten des Auftraggebers auf physischen Datenträgern erfolgt nicht. Zum Zwecke der Abrechnung der Dienstleistung werden Abrechnungsdaten über eine verschlüsselte Verbindung in die Buchhaltungssysteme des Auftragnehmers überführt.

2.2. Eingabekontrolle

Der Auftragnehmer hat die Nachvollziehbarkeit bzw. Dokumentation der Datenverarbeitung zu gewährleisten. Hierzu werden alle Eingaben in die Systeme und Anwendungen durch den Auftragnehmer protokolliert. Die Protokolle werden archiviert und nach Zweckerreichung oder gesetzlichen Vorgaben gelöscht. Die OpenProject-Applikation unterstützt die Eingabe und Änderung der eigenen Daten ausschließlich über hierzu vorgesehene Nutzeroberflächen und Schnittstellen gemäß einem detaillierten Rollen- und Berechtigungskonzept. Bei vielen Objekten kann der Auftraggeber auch über die Weboberfläche die Änderungshistorie von Daten einsehen (z.B. Arbeitspakete, Wiki-Seiten, SCM-Repositories).

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

3.1. Verfügbarkeitskontrolle

Der Auftragnehmer hat personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen. Hierzu ist die Architektur der datenverarbeitenden Systeme des Auftragnehmers einschließlich der Netzwerkinfrastruktur, der Stromversorgung und der Anbindung an das Internet redundant ausgelegt.

Zur Vermeidung von Datenverlusten ist ein umfangreiches Sicherungs- und Wiederherstellungs-Konzept implementiert. Die Daten des Auftraggebers werden kontinuierlich über einen Replikationsmechanismus in separaten

Verfügbarkeitszone gesichert. Zusätzlich werden täglich vollständige Sicherungen aller Systeme und Daten vorgenommen.

Die Systeme und Anwendungen werden laufend hinsichtlich Verfügbarkeit, Funktionstüchtigkeit, Sicherheit und Auslastung überwacht. Es existiert ein schriftlicher Notfallplan, um die Sicherungen bei Verlust oder Zerstörung zurückzuspielen.

3.2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Nach einem eingetretenen Datenverlust muss eine rasche Wiederherstellbarkeit der Daten gewährleistet werden.

Zum Schutz gegen den Verlust von Kundendanten wird eine Kombination von redundaten Systemen sowie Backup-Lösungen eingesetzt. Alle Daten werden mindestens einmal täglich gesichert. Im Fall eines Datenverlustes können diese Daten aus den erstellten Backups wiederhergestellt werden. Die Speicherung der Daten erfolgt in geographisch unabhängigen Standorten.

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

Belastbarkeit meint die Fähigkeit, Angriffen zu widerstehen bzw. Systeme nach einer Attacke zügig wieder in funktionsfähigen Zustand zu bringen.

Die technischen Systeme der OpenProject-Plattform sind in der Lage die erwartbaren Störereignisse zu bewältigen, ohne dass deren Funktionsfähigkeit wesentlich beeinträchtigt werden. Die IT Systeme werden kontinuierlich gehärtet, um gegen bekannte Angriffe, wie beispielsweise Denial-of-Service-Attacken geschützt zu sein.

Zusätzlich ist jede wesentliche Komponente redundant ausgelegt, so dass im Falle einer Störung ein automatischer Wechsel auf eine störungsfreie Komponente erfolgt. Auch können zusätzliche Kapazitäten flexibel getauscht oder erweitert werden.

Die OpenProject-Plattform verfügt über eine moderne Schichten-Architektur. Hiebei sind die Zugriffe der Aspekte technisch über Netztrennungen so eingeschränkt, dass beispielsweise das Datenbank-Management-System nicht aus dem Internet erreicht werden kann, sondern lediglich die Load-Balancer.

Es bestehen Notfallpläne, welche im Falle einer Störung exakte Handlungsanweisungen für die Wiederherstellung des gewünschten Zustandes geben. Diese Notfallpläne sowie die Schutzkonzepte werden kontinuierlich geprüft und deren Anwendung regelmäßig von den verantwortlichen Mitarbeitern trainiert.

5. Datenschutz-Management

5.1. Verantwortliche Ansprechpartner des Auftragnehmers

Herr Ingo Wolff (Datenschutzbeauftragter)

Tacticx GmbH

Walbecker Straße 53

47608 Geldern

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

Zur Gewährleistung der Sicherheit der Datenverarbeitung muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der ergriffenen technischen und organisatorischen Maßnahmen implementiert sein.

Die Umsetzung dieser Maßnahme erfolgt mit Hilfe eines Datenschutz-Management-Systems. Im Rahmen eines kontinuierlichen Verbesserungsprozesses werden die getroffenen technischen und organisatorischen Maßnahmen auf deren Wirksamkeit geprüft und optimiert. Als Teil dieser Maßnahmen werden regelmäßige Audits durch einen externen akkreditierten Fachgutachter durchgeführt.

5.3. Incident-Response-Management; Meldeweg

Es muss gewährleistet sein, dass bei Datenschutzverstößen bzw. des Verdachts von Datenschutzverstößen der Auftragnehmer unverzüglich den Auftraggeber informiert.

Alle Vertragspartner sind vertraglich verpflichtet Datenschutzvorfälle innerhalb der gesetzlichen Fristen zu melden. Interne Prozesse stellen sicher, dass im Falle eines Datenschutzvorfalls die Einbindung des Datenschutzbeauftragten gewährleistet ist.

5.4. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Durch datenschutzfreundliche Voreinstellungen ist zu gewährleisten, dass nur personenbezogenen Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden.

Nach Ablauf der Testphase sowie nach Beendigung des Vertragsverhältnisses werden die erfassten Kundendaten automatisch innerhalb von drei Monaten gelöscht. Zusätzlich dazu kann der Kunde selbständig einzelne Nutzer innerhalb seiner OpenProject-Installation löschen. Hierbei werden folgende personenbezogenen Daten gelöscht:

- Vor- und Zuname
- E-Mail-Adresse

- Telefonnummer
- Nutzername
- Nutzer-Profilbild (Avatar-Bild)

Die erstellten Daten, wie beispielsweise Kommentare zu Arbeitspaketen werden nach dem Löschen einem anonymisierten Nutzer zugeordnet.
Datenschutzfreundliche Einstellungen werden bei Entwicklung und Betrieb der Software berücksichtigt.

5.5. Auftragskontrolle

Der Auftragnehmer verarbeitet die eingereichten Daten gemäß dem geschlossenen Vertrag und gewährleistet hierbei die gesetzlichen Vorschriften und per Vertrag definierten Anforderungen im Rahmen der Weisungen des Auftraggebers. Die OpenProject-Plattform verfügt über eine Administrationsoberfläche, über die der Auftraggeber sein Kundenkonto verwalten kann. Der Auftraggeber legt seine Zugangsdaten bei der initialen Erstellung in seinem Nutzerkonto selbst fest. Nur wer über diese Zugangsdaten verfügt, kann im Rahmen der zugeordneten Berechtigung Kundendaten eingeben, verändern oder löschen. Für sonstige Aufträge, welche der Auftraggeber nicht selbständig über die Administrationsoberfläche durchführen kann, gilt die Schriftform.

Anlage 2: Liste der eingesetzten Unterauftragnehmer

Der Auftraggeber stimmt der Einbeziehung der in dieser Anlage genannten Unterauftragnehmer des Auftragnehmers zu.

Unterauftragnehmer	**Gegenstand der Beauftragung**	**Darlegung der Gewährleistung des Schutzniveaus**
Amazon Web Services Inc. 410 Terry Avenue North, Seattle WA 98109-5210, USA	Infrastructure-as-a-Service	Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und DSG-VO)
Google Inc. 1600 Amphitheatre Parkway Mountain View CA 94043, USA	Analyse des Nutzer-Zugriffsverhaltens zur Produktoptimierung	Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und DSG-VO)
Cyril Rohr EIRL 99 rue de la rabine 35510 CESSON-SÉVIGNÉ, France	Consulting DevOps und Continuous Delivery, Erstellung von Software-Paketen	Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und DSG-VO)
Forkmerge SL C/ Guillem Massot, 44, Piso 3 07003 Palma de Mallorca, Spain	Consulting Software Entwicklung	Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und DSG-VO)
Thomas Gerstmann Saastraße 84 52062 Aachen, Germany	Consulting User Experience	Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und DSG-VO)
MessageBird B.V. Baarsjesweg 285-H 1058 AE Amsterdam, Netherlands	Übermittlung von Authentifizierungstoken per SMS oder Sprachanruf für die Zweifaktor-Authentifizierung	Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und DSG-VO)
Mailchimp	Versand von E-Mail-Benachrichtigungen (Produk-	Standarddatenschutzklauseln

The Rocket Science Group, LLC 675 Ponce De Leon Ave NE Atlanta, GA 30308, USA	tinformationen, Newsletter, Sicherheits-Benachrichtigungen etc.)	(Art. 46 Abs. 2 litt. c und DSG-VO)
PipeDrive 460 Park Ave South New York, NY 10016, USA	Verwaltung von Angebots-anfragen von Kunden	Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und DSG-VO)
Sendgrid Inc. 1801 California St Denver, CO 80202, USA	Versand von E-Mail-Benachrichtigungen	Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und DSG-VO)