Version: November 2025

AUFTRAGSVERARBEITUNGSVERTRAG
COSUNO VENTURES GMBH

zwischen

Cosuno Ventures GmbH

(nachfolgend „**Auftragsverarbeiter**")

und

Kunde

(nachfolgend "**Kunde"**)

(der Auftragsverarbeiter und der Kunde nachfolgend die „**Parteien**" bzw. jeweils eine „**Partei**")

1. Vertragsgegenstand

Bei der Erfüllung des Vertrages zwischen den Parteien über die Bereitstellung der Software des Auftragsverarbeiters für den Kunden (nachfolgend der „**Hauptvertrag**“) ist es notwendig oder möglich, dass der Auftragsverarbeiter mit personenbezogenen Daten umgeht, in Bezug auf welche der Kunde als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften agiert (nachfolgend die „**Kundendaten**“). Dieser Vertrag (nachfolgend der „**Auftragsverarbeitungsvertrag**“) konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Nutzung von Kundendaten durch den Auftragsverarbeiter bei der Erbringung von vertraglichen Leistungen.

2. Umfang der Auftragsverarbeitung

2.1 Der Auftragsverarbeiter verarbeitet die Kundendaten im Auftrag und nach Weisung des Kunden in Übereinstimmung mit Art. 28 Datenschutz-Grundverordnung (nachfolgend „**DSGVO**“). Der Kunde bleibt Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

2.2 Art, Umfang und Zweck der Verarbeitung der Kundendaten durch den Auftragsverarbeiter erfolgen entsprechend den in **Anlage 1** zu diesem Auftragsverarbeitungsvertrag enthaltenen Festlegungen; die Verarbeitung bezieht sich auf die dort spezifizierte Art der personenbezogenen Daten und den dort bestimmten Kreis der Betroffenen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags.

2.3 Die Verarbeitung der Kundendaten durch den Auftragsverarbeiter erfolgt grundsätzlich innerhalb der Europäischen Union oder eines anderen Vertragsstaates des Europäischen Wirtschaftsraums (EWR). Der Auftragsverarbeiter ist jedoch berechtigt, Kundendaten außerhalb des EWR gemäß den Bestimmungen dieses Auftragsverarbeitungsvertrages zu verarbeiten, wenn er den Kunden vorab über den Ort der Datenverarbeitung informiert und wenn die Anforderungen des Kapitels V der DSGVO erfüllt sind.

3. Weisungsbefugnisse des Kunden

3.1 Der Auftragsverarbeiter verarbeitet die Kundendaten gemäß den Weisungen des Kunden – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern der Auftragsverarbeiter nicht gesetzlich anderweitig verpflichtet ist. Im letzteren Fall informiert der Auftragsverarbeiter den Kunden vor der Verarbeitung über diese gesetzliche Verpflichtung, es sei denn, das Gesetz verbietet diese Mitteilung aufgrund eines wichtigen öffentlichen Interesses.

3.2 Die Weisungen des Kunden sind in den Bestimmungen dieses Auftragsverarbeitungsvertrags grundsätzlich abschließend festgelegt und dokumentiert. Individuelle Weisungen, die von den Bestimmungen dieses Auftragsverarbeitungsvertrags abweichen oder zusätzliche Anforderungen stellen, die über die im Hauptvertrag vereinbarte Leistung hinausgehen und nicht erforderlich sind, um Rechtsverstöße im Bereich des Auftragsverarbeiters zu verhindern oder abzustellen, sind angemessen zu

vergüten. Der Auftragsverarbeiter informiert den Kunden in dem Fall vorab über die Entstehung von Kosten bei Ausführung der Weisung.

3.3 Der Auftragsverarbeiter stellt sicher, dass die Kundendaten gemäß den Weisungen des Kunden verarbeitet werden. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Kunden gegen diesen Auftragsverarbeitungsvertrag oder geltendes Datenschutzrecht verstößt, ist er nach entsprechender Mitteilung an den Kunden berechtigt, die Ausführung der Weisung auszusetzen, bis der Kunde die Weisung bestätigt. Die Parteien vereinbaren, dass die alleinige Verantwortung für die Datenschutzkonformität der Weisungen beim Kunden liegt.

4. Rechtliche Verantwortlichkeit des Kunden

4.1 Der Kunde ist allein verantwortlich für die Zulässigkeit der Verarbeitung der Kundendaten und für die Wahrung der Rechte der betroffenen Personen im Verhältnis zwischen den Parteien. Sollten Dritte Ansprüche gegen den Auftragsverarbeiter aus der vertragsgemäßen Verarbeitung von Kundendaten geltend machen, stellt der Kunde den Auftragsverarbeiter auf erstes Anfordern von allen diesen Ansprüchen frei, es sei denn, der Anspruch des Dritten resultiert offensichtlich aus einem Gesetzes- oder Vertragsverstoß des Auftragsverarbeiters.

4.2 Dem Kunden obliegt es, dem Auftragsverarbeiter die Kundendaten rechtzeitig zur vertragsgemäßen Leistungserbringung zur Verfügung zu stellen und er ist für die Qualität der Kundendaten verantwortlich. Der Kunde hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Ergebnisse des Auftragsverarbeiters Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen oder seine Weisungen feststellt.

5. Anforderungen an Personal

5.1 Der Auftragsverarbeiter verpflichtet alle an der Verarbeitung von Kundendaten beteiligten Personen zur Vertraulichkeit in Bezug auf die Verarbeitung von Kundendaten.

6. Sicherheit der Verarbeitung

6.1 Der Auftragsverarbeiter ergreift die erforderlichen geeigneten technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO unter Berücksichtigung des Standes der Technik, der Durchführungskosten und der Art, des Umfangs, der Umstände und Zwecke der Kundendaten sowie der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen, um ein dem Risiko angemessenes Schutzniveau der Kundendaten zu gewährleisten. Die umgesetzten technischen und organisatorischen Maßnahmen umfassen die in **Anlage 2** aufgeführten Maßnahmen.

6.2 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet,

alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

7. Einsatz von Unterauftragsverarbeitern

7.1 Der Kunde erteilt dem Auftragsverarbeiter grundsätzlich die Erlaubnis, Unterauftragsverarbeiter mit der Verarbeitung von Kundendaten zu beauftragen. Unterauftragsverarbeiter, die zum Zeitpunkt des Abschlusses dieses Auftragsverarbeitungsvertrags beschäftigt sind, sind in **Anlage 3** aufgeführt.

7.2 Der Auftragsverarbeiter wird den Kunden über beabsichtigte Änderungen im Zusammenhang mit der Einbeziehung oder dem Austausch von Unterauftragsverarbeitern informieren (Angabe von Unternehmen, Anschrift und stichwortartige Beschreibung der Datenverarbeitung). Der Kunde hat im Einzelfall das Recht, dem Einsatz eines potenziellen Unterauftragsverarbeiters zu widersprechen. Ein Widerspruch kann vom Kunden aus sachlichen Gründen erhoben werden, die dem Auftragsverarbeiter mitzuteilen sind. Eine Mitteilung über den Einsatz neuer Unterauftragsverarbeiter erfolgt durch den Auftragsverarbeiter spätestens 14 Tage vor dem geplanten Einsatz des Unterauftragsverarbeiters. Sofern der Kunde nicht innerhalb von 14 Tagen nach Erhalt der Mitteilung widerspricht, gilt der Unterauftragsverarbeiter als genehmigt. Widerspricht der Kunde, ist der Verarbeiter berechtigt, den Hauptvertrag und diesen Auftragsverarbeitungsvertrag mit einer Frist von drei Monaten zum Ende eines Monats zu kündigen.

7.3 Die Vereinbarung zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter muss dem Unterauftragsverarbeiter die gleichen Verpflichtungen auferlegen wie die, die dem Auftragsverarbeiter im Rahmen dieses Auftragsverarbeitungsvertrags obliegen. Die Parteien vereinbaren, dass diese Anforderung erfüllt ist, wenn die Vereinbarung ein diesem Auftragsverarbeitungsvertrag entsprechendes Schutzniveau aufweist.

7.4 Vorbehaltlich der Erfüllung der Anforderungen des Abschnitts 2.3 dieses Auftragsverarbeitungsvertrages gelten die Bestimmungen dieses Abschnitts 7 auch, wenn ein Unterauftragsverarbeiter in einem Drittland beteiligt ist. Sofern die Verarbeitung nicht auf Grundlage eines von der EU-Kommission erlassenen Angemessenheitsbeschlusses erfolgt, vereinbaren die Parteien, dass der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der DSGVO sicherstellen können, indem sie die jeweils aktuell von der EU-Kommission gemäß Artikel 46 Absatz 2 der DSGVO erlassenen Standardvertragsklauseln verwenden.

8. Rechte der betroffenen Personen

8.1 Der Auftragsverarbeiter wird den Kunden nach Möglichkeit mit technischen und organisatorischen Maßnahmen unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III des DSGVO genannten Rechte der betroffenen Personen nachzukommen. Aufwände, die dem Auftragsverarbeiter infolge der

Unterstützung des Kunden entstehen, sind angemessen zu vergüten, es sei denn, die Unterstützungsleistungen wurden aufgrund eines Verstoßes des Auftragsverarbeiters gegen die einschlägigen Datenschutzbestimmungen oder diesen Auftragsverarbeitungsvertrag erforderlich.

8.2 Soweit eine betroffene Person einen Antrag auf Wahrnehmung ihrer Rechte direkt an den Verarbeiter richtet, wird der Auftragsverarbeiter diesen Antrag rechtzeitig an den Kunden weiterleiten.

9. Melde- und Unterstützungspflichten des Auftragsverarbeiters

9.1 Der Auftragsverarbeiter unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten. Dem Auftragsverarbeiter werden die ihm in diesem Zusammenhang entstandenen und gegenüber dem Kunden nachgewiesenen Aufwendungen und Kosten angemessen vergütet, es sei denn, die Meldepflicht des Kunden bzw. die Unterstützungsleistungen des Auftragsverarbeiters resultieren aus einem Verstoß des Auftragsverarbeiters gegen die einschlägigen Datenschutzbestimmungen oder diesen Auftragsverarbeitungsvertrag.

9.2 Soweit der Kunde aufgrund einer Verletzung des Schutzes der Kundendaten einer gesetzlichen Meldepflicht unterliegt (insbesondere gemäß Art. 33, 34 DSGVO), wird der Auftragsverarbeiter den Kunden rechtzeitig über meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren.

10. Löschung und Rückgabe von Kundendaten

10.1 Nach Abschluss der Erbringung der Verarbeitungsleistungen wird der Auftragsverarbeiter nach Wahl des Kunden,

a) die Kundendaten entweder löschen oder zurückgeben; und

b) bestehende Kopien löschen

es sei denn, der Auftragsverarbeiter ist im Sinne des Art. 28 (3) 2 lit. g DSGVO gesetzlich zur weiteren Speicherung der Kundendaten verpflichtet.

11. Nachweise und Überprüfungen

11.1 Der Auftragsverarbeiter stellt dem Kunden auf Verlangen alle Informationen zur Verfügung, die zum Nachweis der Erfüllung seiner Verpflichtungen aus diesem Auftragsverarbeitungsvertrag und unmittelbar aus der DSGVO hervorgehenden Pflichten erforderlich sind.

11.2 Der Kunde ist berechtigt, den Auftragsverarbeiter hinsichtlich der Einhaltung der Bestimmungen dieses Auftragsverarbeitungsvertrags, insbesondere der Durchführung der technischen und organisatorischen Maßnahmen, zu überprüfen (einschließlich

Vor-Ort-Kontrollen).

11.3 Die Durchführung von Überprüfungen nach Ziffer 11.2 erfolgt grundsätzlich innerhalb der üblichen Geschäftszeiten (Montag bis Freitag von 10 bis 18 Uhr) und ist in der Regel nach Ziff. 11.5 rechtzeitig anzukündigen, um übermäßige Beeinträchtigungen des Geschäftsablaufs zu vermeiden. Das Betreten der Geschäftsräume des Auftragsverarbeiters erfolgt unter strikter Geheimhaltung der Geschäfts- und Betriebsgeheimnisse des Auftragsverarbeiters, wobei die Geheimhaltungsverpflichtung einer etwaigen bestehenden Nachweiserbringungspflicht gegenüber der Aufsichtsbehörde oder den Betroffenen nicht entgegensteht – vertrauliche Informationen im Sinne der Ziff. 11.4 sind insoweit in dem erforderlichen Umfang unkenntlich zu machen, sofern die Mitteilung des Prüfergebnisses als solches nicht ohnehin genügt. Die Überprüfung des Auftragsverarbeiters erfolgt auf Kosten des Kunden, sofern die Überprüfung nicht aufgrund eines Gesetzes- oder Vertragsverstoßes des Auftragsverarbeiters erforderlich wurde.

11.4 Der Auftragsverarbeiter ist berechtigt, unter Berücksichtigung der gesetzlichen Verpflichtungen des Kunden Informationen nicht preiszugeben, die im Hinblick auf die Geschäftstätigkeit des Auftragsverarbeiters sensibel sind oder wenn der Auftragsverarbeiter durch seine Preisgabe gegen gesetzliche oder andere vertragliche Bestimmungen verstoßen würde. Der Kunde ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragsverarbeiters, Kosteninformationen, Qualitätskontroll- und Vertragsmanagementberichten oder zu anderen vertraulichen Daten des Auftragsverarbeiters zu erhalten, die für die vereinbarten Prüfungszwecke nicht unmittelbar relevant sind.

11.5 Der Kunde hat den Auftragsverarbeiter rechtzeitig (in der Regel mindestens zwei Wochen im Voraus, sofern dies den Kontrollzweck nicht gefährdet) über alle Umstände im Zusammenhang mit der Durchführung der Überprüfung zu informieren. Solange kein triftiger Grund vorliegt, darf der Kunde nicht mehr als eine Überprüfung pro Kalenderjahr durchführen. Ein triftiger Grund ist insbesondere bei Vorliegen eines begründeten Verdachts auf eine Datenschutzverletzung gegeben.

11.6 Beauftragt der Kunde einen Dritten mit der Durchführung der Überprüfung, so hat der Kunde den Dritten in gleicher Weise schriftlich zu verpflichten, wie der Kunde gegenüber dem Auftragsverarbeiter nach diesem Abschnitt 11 verpflichtet ist. Darüber hinaus verpflichtet der Kunde den Dritten durch schriftliche Vereinbarung zur Geheimhaltung und Vertraulichkeit, es sei denn, der Dritte unterliegt einer beruflichen Geheimhaltungspflicht. Auf Verlangen des Auftragsverarbeiters hat der Kunde ihm unverzüglich die Verpflichtungs- und Geheimhaltungsvereinbarungen mit dem Dritten vorzulegen. Der Kunde darf keine unmittelbaren Wettbewerber des Auftragsverarbeiters mit der Durchführung der Überprüfung beauftragen.

11.7 Bei der Entscheidung über die Durchführung einer Überprüfung nach Ziff. 11.2 kann der Kunde einschlägige Zertifizierungen des Auftragsverarbeiters, insbesondere die Vorlage einer entsprechenden aktuellen Stellungnahme oder eines Berichts einer unabhängigen

Behörde (z.B. Wirtschaftsprüfer, Revisionsabteilung, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzprüfer oder Qualitätsprüfer) oder einer geeigneten Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit (nachfolgend der „**Prüfungsbericht**“) berücksichtigen, wenn es der Prüfungsbericht dem Kunden in angemessener Weise ermöglicht, sich von der Einhaltung der in diesem Auftragsverarbeitungsvertrag enthaltenen vertraglichen Verpflichtungen durch den Auftragsverarbeiters zu überzeugen.

12. Vertragslaufzeit und Kündigung

Die Laufzeit und Kündigung dieses Auftragsverarbeitungsvertrags richten sich nach den Bestimmungen der Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags führt automatisch zur Kündigung dieses Auftragsverarbeitungsvertrags. Eine gesonderte Kündigung dieses Auftragsverarbeitungsvertrags ist nicht erforderlich.

13. Haftung

13.1 Die Haftung des Auftragsverarbeiters im Rahmen dieses Auftragsverarbeitungsvertrags richtet sich nach den im Vertrag vorgesehenen Haftungsausschlüssen und -beschränkungen. Für den Fall, dass Haftungsfragen im Vertrag nicht vollständig geregelt sind, greifen die Haftungsklauseln nach Art. 82 DSGVO.

13.2 Der Kunde verpflichtet sich, den Auftragsverarbeiter auf erstes Anfordern in der Höhe von allen dem Auftragsverarbeiter auferlegten Geldbußen freizustellen, welche dem Teil der Verantwortlichkeit des Kunden für die mit der Geldbuße geahndete Verletzung entspricht.

14. Schlussbestimmungen

14.1 Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden oder eine Regelungslücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine rechtlich zulässige Bestimmung zu ersetzen, die dem Zweck der unwirksamen Bestimmung am nächsten kommt und damit die Anforderungen des Art. 28 DSGVO erfüllt.

14.2 Im Falle von Widersprüchen zwischen diesem Auftragsverarbeitungsvertrag und anderen Vereinbarungen der Parteien, insbesondere dem Hauptvertrag, haben die Bestimmungen dieses Auftragsverarbeitungsvertrags Vorrang.

Anlagen:

Anlage 1: Weitere Informationen zur Verarbeitung von Kundendaten

Anlage 2: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Anlage 3: Unterauftragsverarbeiter

Anlage 1
Weitere Informationen zur Verarbeitung von Kundendaten

1	Zweck und Umfang der Datenverarbeitung	Bereitstellung der Cosuno-Plattform als Software-as-a-Service Tool und (soweit vorhanden) weitere im Hauptvertrag genannte Verarbeitungszwecke. Die Cosuno-Plattform dient dazu, dem Kunden die intelligente Verwaltung der Beauftragung von Nachunternehmern in Bauprojekten zu ermöglichen.
2	Art der personenbezogenen Daten	Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten
3	Kategorien betroffener Personen	Mitarbeiter des Kunden; Zulieferer des Kunden, Endkunden des Kunden; weitere im Hauptvertrag genannte Kategorien betroffener Personen (falls vorhanden)

Anlage 2
Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

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

1.1 Zutrittskontrolle

Der Auftragnehmer ergreift Maßnahmen, um den unbefugten Zutritt zu Datenverarbeitungsanlagen zu sichern.

In den Büroräumen des Auftragnehmers sind unter anderem folgende Maßnahmen umgesetzt:

Technische Maßnahmen	- Manuelles Schließsystem - Sicherheitsschlösser - Alarmanlage - Klingelanlage mit Kamera
Organisatorische Maßnahmen	- Schlüsselregelung und Schlüsselbuch - Besucher nur in Begleitung durch Mitarbeiter - Sorgfältige Auswahl von Reinigungspersonal

Die produktiven Systeme zur Verarbeitung personenbezogener Daten werden nicht in den Büroräumen des Auftragnehmers, sondern ausschließlich in den Rechenzentren von sorgfältig ausgewählten Unterauftragnehmern betrieben.

Dazu gehören Hosting-Anbieter wie AWS (Amazon Web Services) und GCP (Google Cloud Platform) sowie alle weiteren eingesetzten Unterauftragnehmer, die personenbezogene Daten im Auftrag verarbeiten—siehe Anlage 3.

1.2 Zugangs- und Benutzerkontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um die unbefugte Systembenutzung von Datenverarbeitungsanlagen zu sichern.

Technische Maßnahmen	- Authentifizierung mit Benutzername und Passwort - Multi-Faktor-Authentifizierung - Verschlüsselung von Datenträgern - Einsatz von Anti-Viren-Software

	- Einsatz von Firewalls - Einsatz von Password Manager - Automatische Desktopsperre bei Inaktivität
Organisatorische Maßnahmen	- Berechtigungskonzept basiert auf den Need-to-know- und Least-Privilege-Prinzipien - Eindeutige Zuordnung von Benutzerprofilen zu IT-Systemen - Unmittelbare Löschung des Zugangs nach Ausscheiden eines Mitarbeiters - Unternehmensweite Passwortrichtlinie inkl. Passwortlänge und -wechselzyklus - Clean Desk Policy

1.3 Zugriffs, Daten- und Speicherkontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems zu verhindern.

Technische Maßnahmen	- Einsatz von Aktenvernichtern - Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) - Physische Löschung von Datenträgern vor einer Wiederverwendung - Protokollierung von Zugriffen auf Anwendungen, insbes. bei der Eingabe, Änderung und Löschung von Daten - Verwendung von Version Control-Systemen (VCS) und Code Review-Prozessen bei Softwareänderungen
Organisatorische Maßnahmen	- Berechtigungskonzept basiert auf den Need-to-know- und Least-Privilege-Prinzipien - Minimale Anzahl an Administratoren - Verwaltung der Benutzerrechte durch definierte Administratoren - Unternehmensweite Passwortrichtlinie inkl.

	Passwortlänge und -wechselzyklus - Sichere Aufbewahrung von Datenträgern - Protokollierung der Vernichtung von Daten

1.4 Trennungskontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, sicherzustellen.

Technische Maßnahmen	- Trennung von Produktiv-, Test- und Entwicklungsumgebung - Getrennte Speicherung von Daten die zu unterschiedlichen Zwecken verarbeitet werden - Mandantenfähigkeit relevanter Anwendungen
Organisatorische Maßnahmen	- Berechtigungskonzept basiert auf den Need-to-know- und Least-Privilege-Prinzipien - Klar dokumentierte, begrenzte Vergabe von Zugriffsrechten auf Datenbanken - Dokumentation der Verarbeitungszwecke für alle Kategorien gespeicherter Daten

1.5 Pseudonymisierung

Der Auftragnehmer setzt unter anderem die folgenden Maßnahmen ein, um sicherzustellen, dass im Falle einer Pseudonymisierung bestimmter Daten diese Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Technische Maßnahmen	- Im Falle einer Pseudonymisierung, getrennte Aufbewahrung der Zuordnungsdaten in einem separaten, abgesicherten System
Organisatorische Maßnahmen	- Interne Richtlinien, in welchen Fällen und auf welche Art und Weise eine Pseudonymisierung bestimmter Datensätze zu erfolgen hat

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

2.1 Weitergabekontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport zu verhindern.

Technische Maßnahmen	- Verschlüsselte Datenübertragung (TLS/HTTPS) - Systemseitige Protokollierung von Zugriffen und abgerufenen Daten - Sichere Transportbehälter und -verpackungen beim physischen Transport von Daten
Organisatorische Maßnahmen	- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen - Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge - Weitergabe in anonymisierter oder pseudonymisierter Form sofern möglich - Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen

2.2 Eingabekontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um festzustellen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten - Manuelle oder automatisierte Kontrolle der Protokolle
Organisatorische Maßnahmen	- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle

	Benutzernamen (nicht Benutzergruppen) - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis des Berechtigungskonzepts - Löschkonzept mit klaren Zuständigkeiten und Protokollierung

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

3.1 Verfügbarkeitskontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen.

Technische Maßnahmen	- Nutzung von ausgelagerten Rechenzentren, die nach ISO 27001 zertifiziert sind und umfassende Maßnahmen einsetzen, um ein hohes Maß an Verfügbarkeit zu gewährleisten (Brandschutz, Klimaanlage, unterbrechungsfreie Stromversorgung usw.) - Redundante Systemarchitektur - Flexible Skalierbarkeit der IT-Infrastruktur - Automatisierte Backup-Prozesse - Kontinuierliche Überwachung der IT-Systeme (Monitoring)
Organisatorische Maßnahmen	- Dokumentiertes Backup- und Recovery-Konzept - Kontrolle der Sicherungsvorgänge - Regelmäßige Tests zur Datenwiederherherstellung und Protokollierung der Ergebnisse - Aufbewahrung von Backups an einem sicheren, ausgelagerten Ort - Dokumentierter Notfallplan

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

4.1 Datenschutz-Maßnahmen

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um die innerbetriebliche Organisation so zu gestalten, sodass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Technische Maßnahmen	- Software-Lösungen für Datenschutz-Management im Einsatz - Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter
Organisatorische Maßnahmen	- Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen, mindestens jährlich - Schulung der Mitarbeiter zu Datenschutz und DSGVO, mit Protokollierung der Teilnahme - Jährliche Wiederholung der Schulungen - Protokollierte Verpflichtung der Mitarbeiter auf Vertraulichkeit - Schriftliche Bestellung eines Datenschutzbeauftragten - Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener

4.2 Incident-Response-Management

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um einen DSGVO-konformen Umgang mit IT-Sicherheitsvorfällen sicherzustellen.

Organisatorische Maßnahmen	- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und Datenpannen, auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörden - Dokumentierte Vorgehensweise zum Umgang mit

	Sicherheitsvorfällen - Einbindung des Datenschutzbeauftragten bei Sicherheitsvorfällen und Datenpannen - Ausführliche Dokumentation von Sicherheitsvorfällen und Datenpannen - Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um die Verarbeitung nur erforderlicher personenbezogener Daten durch Voreinstellung sicherzustellen.

Organisatorische Maßnahmen	- Keine Erhebung personenbezogener Daten, die nicht für den jeweiligen Zweck erforderlich sind - Datenschutzfreundliche Gestaltung der Voreinstellungen von Produkten und Diensten, bereits vor ihrer ersten Inanspruchnahme

4.4 Auftragskontrolle

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen, um die weisungsgemäße Verarbeitung von Daten im Auftrag sicherzustellen.

Organisatorische Maßnahmen	- Auswahl von Dienstleistern unter Sorgfaltsgesichtspunkten in Bezug auf Datenschutz und Datensicherheit - Vorherige Prüfung der vom Dienstleister getroffenen Sicherheitsmaßnahmen und deren Dokumentation - Abschluss von Vereinbarungen zur Auftragsverarbeitung (AVV) mit Dienstleistern - Regelmäßige Überprüfung des Dienstleisters und seines Schutzniveaus

Anlage 3
Unterauftragsverarbeiter

Nr.	Name des Unterauftragsverarbeiters	Beschreibung der Verarbeitung durch den Unterauftragsverarbeiter	Ort der Datenverarbeitung
1	Amazon Web Services EMEA SARL	Cloud Hosting	Deutschland
2	DanglIT GmbH	Verarbeitung von Leistungsverzeichnissen	Deutschland
3	Datadog, Inc.	Speicherung von technischen Logs, Monitoring	Deutschland
4	dbt Labs, Inc.	Bereitstellung von Berichten und Datenanalysen	USA (Grundlage: Angemessenheitsbeschluss nach Art. 45 DSGVO; EU-U.S. Data Privacy Framework)
5	Functional Software Inc	Technisches Fehlertracking	Deutschland
6	Google LLC	Cloud Hosting	Deutschland
7	Intercom, Inc.	Live-Chat mit Kundensupport	USA (Grundlage: Angemessenheitsbeschluss nach Art. 45 DSGVO; EU-U.S. Data Privacy Framework)
8	Joincube, Inc.	Anzeigen von Neuigkeiten im Produkt	Belgien (EU)
9	Sinch AB (Mailjet)	Versand von E-Mails	Deutschland / Belgien (EU)
10	Estuary Technologies, Inc.	Bereitstellung von Berichten und Datenanalysen	Deutschland
11	Catamorphic, Co. dba LaunchDarkly	Technische Steuerung von Produktfunktionen	USA (Grundlage: Angemessenheitsbeschluss nach Art. 45 DSGVO; EU-U.S. Data Privacy Framework)