Vereinbarung zur Auftragsverarbeitung

Version 2.0.0 – Stand: 04.11.2026

zwischen

dem Kunden gemäß Plattformvertrag
– nachfolgend „Verantwortlicher“ –

und

Loopback GmbH
Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
vertreten durch den Geschäftsführer Jonathan Bouillon
– nachfolgend „Auftragsverarbeiter“ –

– beide nachfolgend gemeinsam „Vertragsparteien“ –

Präambel

Die Vertragsparteien haben einen Vertrag über die Nutzung der Loopback-Plattform nach den Allgemeinen Geschäftsbedingungen geschlossen; dieser umfasst den Plattformvertrag, die gebuchten Services, die jeweiligen Leistungsbeschreibungen und den Leistungsanhang sowie etwaige Individualvereinbarungen („Leistungsvereinbarung“). Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, „DSGVO“) und des Bundesdatenschutzgesetzes („BDSG“) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

Die Vereinbarung wird durch die folgenden Anhänge konkretisiert. Diese sind Bestandteil der Vereinbarung und haben für die ausgewiesenen Themen vorrangige Wirkung gegenüber allgemeinen Beschreibungen, sofern ausdrücklich auf sie Bezug genommen wird:

- Anhang A – Technisch-organisatorische Maßnahmen,
- Anhang B – Weitere Auftragsverarbeiter,
- Anhang C – Weisungsberechtigte und Weisungswege.

§ 1 Anwendungsbereich

(1) Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: Verarbeitung) aller personenbezogenen Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind, im Rahmen ihrer Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

(2) Nicht Gegenstand dieser Vereinbarung sind Verarbeitungen, bei denen der Auftragsverarbeiter selbst Verantwortlicher im Sinne der DSGVO ist, insbesondere im Rahmen von Account-Verwaltung und Anmeldung an der Plattform einschließlich der Anmeldung über den Identitätsanbieter des Verantwortlichen, Sicherheits- und Audit-Protokollen der Plattform, Abrechnung, Vertrieb, Website und vergleichbarer eigenständiger Geschäftstätigkeit. Diese Verarbeitungen sind in der Datenschutzerklärung des Auftragsverarbeiters beschrieben.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung bestimmen sich nach der Leistungsvereinbarung. Die Verarbeitung umfasst insbesondere das Hosten, Speichern, Übertragen, Sichern, Überwachen und Löschen von Daten in den vom Verantwortlichen gebuchten Services sowie die Bearbeitung von Supportanfragen. Diese Vereinbarung gilt, solange der Auftragsverarbeiter Daten im Auftrag des Verantwortlichen verarbeitet.

(2) Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung:

- Account-, Kontakt- und Identitätsdaten, die der Verantwortliche in seinen Ressourcen verwaltet (z. B. Benutzer, Service Accounts, Robot Accounts und Rollenzuordnungen in Clustern, Registries oder Anwendungen),
- Authentifizierungs-, Zugriffs- und Auditdaten innerhalb der Ressourcen des Verantwortlichen (z. B. Benutzerkennungen, IP-Adressen und Zeitstempel bei Zugriffen auf Cluster, Registry oder Buckets),
- Betriebs-, System- und Sicherheitsprotokolle (z. B. Kubernetes-Audit-Logs, API-, Administrations- und sonstige System- oder Änderungsprotokolle),
- Telemetrie-, Status- und Protokolldaten angebundener kundeneigener Infrastruktur, die der Loopback Agent übermittelt,
- Sicherungskopien der vom Auftragsverarbeiter betriebenen Komponenten (z. B. Zustand der Kubernetes Control Plane einschließlich darin gespeicherter Secrets und Konfigurationen),
- Support-, Ticket- und sonstige Kommunikationsinhalte, die der Verantwortliche im Rahmen von Support-, Betriebs- oder Incident-Prozessen bereitstellt,
- Kundeninhalte in den vom Verantwortlichen genutzten Services, insbesondere in Clustern, persistenten Volumes, Buckets, Registries, DNS-Zonen, Datenbanken und Anwendungen; diese können je nach Nutzung personenbezogene Daten beliebiger Kategorien enthalten, einschließlich besonderer Kategorien nach Art. 9 DSGVO.

(3) Folgende Kategorien betroffener Personen werden durch die Verarbeitung umfasst:

- Mitarbeitende, Beauftragte, Administratoren und sonstige Nutzer des Verantwortlichen,
- Endnutzer, Kunden oder sonstige Nutzer der vom Verantwortlichen betriebenen oder bereitgestellten Anwendungen und Dienste,
- Beschäftigte im Sinne von § 26 Abs. 8 BDSG, soweit Daten des Verantwortlichen in den verarbeiteten Systemen enthalten sind,
- Ansprechpartner bei Geschäftspartnern, Lieferanten oder sonstigen Dritten des Verantwortlichen, soweit diese Daten vom Verantwortlichen in den verarbeiteten Systemen oder Supportvorgängen bereitgestellt werden.

(4) Die Auswahl der Daten, die der Verantwortliche in die Services einbringt, obliegt allein dem Verantwortlichen. Der Auftragsverarbeiter nimmt vom Inhalt der Kundeninhalte nur Kenntnis, soweit dies zur Leistungserbringung, insbesondere zur Bearbeitung einer Supportanfrage oder zur Abwehr einer Sicherheitsgefahr, erforderlich ist.

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Die Vertragsparteien sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen. Soweit die Services

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

hierfür Funktionen bereitstellen, nimmt der Verantwortliche diese Handlungen selbst über die Plattform oder die API vor.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch geeignete technische und organisatorische Maßnahmen. Wendet sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter, leitet dieser das Ersuchen unverzüglich an den Verantwortlichen weiter.

(3) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht durch das Recht der Union oder des Mitgliedstaates, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(4) Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete Anordnung des Verantwortlichen in Textform oder über die Funktionen der Plattform oder API. Die Weisungen werden zunächst durch die Leistungsvereinbarung festgelegt. Als dokumentierte Weisung gelten außerdem alle Handlungen, die berechtigte Nutzer des Verantwortlichen in der Plattform oder über die API vornehmen, insbesondere das Anlegen, Konfigurieren und Löschen von Ressourcen und die Wahl von Infrastrukturanbieter und Region. Einzelweisungen, die über den Funktionsumfang der Services hinausgehen, sind nur im Rahmen der Leistungsvereinbarung oder nach gesonderter Vereinbarung auszuführen; die Vergütung hierfür richtet sich nach Ziffer 5.8 der AGB.

(5) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie vom Verantwortlichen bestätigt oder geändert wird. Weisungsberechtigte Personen, Empfänger von Weisungen und Informationswege ergeben sich aus Anhang C.

(6) Änderungen des Verarbeitungsgegenstands mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger Zustimmung des Verantwortlichen in Textform erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden außerhalb dokumentierter betrieblicher, sicherheitsbezogener oder technisch erforderlicher Prozesse nicht ohne Wissen des Verantwortlichen erstellt.

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt ihm auf Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung und führt selbst ein Verzeichnis nach Art. 30 Abs. 2 DSGVO.

(8) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese ausschließlich auf Weisung des Verantwortlichen verarbeiten. Die Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters ist nur im Rahmen dokumentierter Remote-Work-Controls nach Anhang A zulässig.

§ 4 Ort der Verarbeitung und Drittlandübermittlung

(1) Die Plattform einschließlich API und Steuerungskomponenten betreibt der Auftragsverarbeiter in Deutschland. Ressourcen des Verantwortlichen werden in der Region verarbeitet, die der Verantwortliche bei der Buchung wählt.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

(2) Eine Verarbeitung in einem Staat außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums oder eine Übermittlung dorthin ist nur zulässig, wenn sie auf einer dokumentierten Weisung des Verantwortlichen beruht oder der Auftragsverarbeiter hierzu durch das Recht der Union oder eines Mitgliedstaats verpflichtet ist, und im Übrigen die Anforderungen des Kapitels V DSGVO eingehalten werden. Wählt der Verantwortliche für eine Ressource eine Region außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, liegt darin eine solche Weisung. Der Auftragsverarbeiter zeigt vor der Buchung das Land der Region an und gibt den Transfermechanismus in Anhang B an.

(3) Für Übermittlungen an weitere Auftragsverarbeiter in Drittländern stellt der Auftragsverarbeiter geeignete Garantien sicher, insbesondere durch einen Angemessenheitsbeschluss oder durch Abschluss der Standardvertragsklauseln der Europäischen Kommission (Modul 3). Soweit erforderlich, führen die Vertragsparteien eine Bewertung der Auswirkungen der Übermittlung durch und vereinbaren ergänzende technische und organisatorische Maßnahmen. Die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung im Übrigen bleiben unberührt.

§ 5 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst die Belehrung über die bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf Informationen zur Verfügung.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen im erforderlichen und zumutbaren Umfang bei der Erfüllung seiner Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei einer Datenschutz-Folgenabschätzung und einer vorherigen Konsultation der Aufsichtsbehörde, soweit die vom Auftragsverarbeiter erbrachten Leistungen oder die von ihm durchgeführten Verarbeitungsvorgänge betroffen sind. Er stellt dem Verantwortlichen auf Anforderung die erforderlichen Informationen über die relevanten Verarbeitungsvorgänge und die getroffenen technischen und organisatorischen Maßnahmen zur Verfügung.

(4) Der Auftragsverarbeiter ist nicht verpflichtet, einen Datenschutzbeauftragten zu benennen. Der Ansprechpartner für Datenschutz ist erreichbar unter support@loopback.cloud. Benennt der Auftragsverarbeiter einen Datenschutzbeauftragten, teilt er dem Verantwortlichen dessen Kontaktdaten mit.

(5) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen von Aufsichtsbehörden oder wenn eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit beim Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht, soweit dieser Auftrag betroffen ist.

§ 6 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in Anhang A niedergelegten technischen und organisatorischen Maßnahmen einschließlich ergänzender cloud- und plattformspezifischer Kontrollen sowie Verfahren zu deren regelmäßiger Überprüfung und Nachweisführung.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf alternative adäquate Maßnahmen umsetzen, sofern das Sicherheitsniveau der in Anhang A festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Vereinbarung und der gesetzlichen Vorgaben sowie für eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich sind. Prüfungen durch den Verantwortlichen oder einen von ihm beauftragten Prüfer, der zur Verschwiegenheit verpflichtet ist und nicht im Wettbewerb mit dem Auftragsverarbeiter steht, erfolgen in der Regel auf dokumentierter Basis, insbesondere durch Bereitstellung einschlägiger Unterlagen, aktueller Testate und vergleichbarer Nachweise, sowie durch Remote-Audits.

(4) Vor-Ort-Prüfungen in den Betriebsstätten des Auftragsverarbeiters sind nach vorheriger angemessener Ankündigung und Abstimmung zulässig, grundsätzlich zu den üblichen Geschäftszeiten und so, dass der Betriebsablauf nicht unangemessen beeinträchtigt wird. Sie sollen in der Regel nicht häufiger als zweimal je Kalenderjahr stattfinden, es sei denn, eine weitergehende Prüfung ist aus sachlich begründetem Anlass erforderlich, insbesondere bei konkreten Anhaltspunkten für Verstöße, Datenschutzvorfällen, behördlichen Maßnahmen oder wesentlichen Änderungen der Verarbeitung oder der technischen und organisatorischen Maßnahmen. Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters sowie Daten und Vertraulichkeitsinteressen anderer Kunden sind angemessen zu schützen. Prüfungen in Rechenzentren von Infrastrukturanbietern richten sich nach deren Bedingungen; der Auftragsverarbeiter stellt hierfür deren Nachweise und Zertifizierungen zur Verfügung.

(5) Soweit Prüfungen über das übliche Maß dokumentarischer Nachweise und angemessener Remote-Prüfungen hinausgehen und dadurch ein erheblicher zusätzlicher Aufwand entsteht, kann der Auftragsverarbeiter eine angemessene Kostenerstattung verlangen, sofern er dies vorab transparent mitgeteilt hat und der Aufwand nicht auf einem von ihm zu vertretenden Anlass beruht.

(6) Der Nachweis von Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch durch aktuelle Testate, Berichte hinreichend qualifizierter und unabhängiger Stellen (z. B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, eine Zertifizierung nach Art. 42 DSGVO oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz oder ISO 27001) erbracht werden. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO und jede andere Aufhebung oder wesentliche Änderung dieser Nachweise.

(7) Der Auftragsverarbeiter ergreift im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherheit der Verarbeitung unter Berücksichtigung des Stands der Technik sowie zur Minderung möglicher nachteiliger Folgen für betroffene Personen.

§ 7 Mitteilung bei Verstößen

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Verletzungen des Schutzes personenbezogener Daten, Verdachtsfälle einer solchen Verletzung, Verstöße gegen diese Vereinbarung oder anwendbare datenschutzrechtliche Vorschriften sowie sonstige Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen, soweit diese für den Verantwortlichen datenschutzrechtlich relevant sein können. Dies gilt insbesondere im Hinblick auf Art. 33 Abs. 2 DSGVO sowie auf die Pflichten des Verantwortlichen nach Art. 33 und 34 DSGVO.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

(2) Die Erstinformation erfolgt unverzüglich, möglichst innerhalb von 24 Stunden nach Bekanntwerden des Vorfalls beim Auftragsverarbeiter, auf Basis des jeweils verfügbaren Kenntnisstands, per E-Mail an die in der Organisation hinterlegte Adresse. Sie enthält, soweit zu diesem Zeitpunkt möglich, mindestens Art und ungefähres Ausmaß des Vorfalls, die betroffenen oder potenziell betroffenen Systeme und Verarbeitungsumgebungen, die betroffenen oder potenziell betroffenen Datenkategorien, bereits ergriffene oder geplante Abhilfemaßnahmen sowie eine erreichbare Kontaktstelle. Weitere Informationen werden ohne unangemessene Verzögerung nachgereicht.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen erforderlichenfalls angemessen bei dessen Pflichten nach Art. 33 und 34 DSGVO. Meldungen an Aufsichtsbehörden oder betroffene Personen für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung nach § 3 vornehmen.

§ 8 Löschung und Rückgabe von Daten

(1) Daten, die im Zusammenhang mit dem Auftragsverhältnis an den Auftragsverarbeiter gelangen, verbleiben im Herrschafts- und Zuordnungsbereich des Verantwortlichen. Dies gilt unbeschadet gesetzlicher Rechte sowie solcher Datenkopien, Protokolle, Sicherungen und Dokumentationen, deren Speicherung zur ordnungsgemäßen Durchführung des Auftrags, zur Datensicherung oder zur Erfüllung gesetzlicher Aufbewahrungspflichten erforderlich ist.

(2) Löscht der Verantwortliche eine Ressource, gilt dies als Weisung zur Löschung der darin gespeicherten Daten. Bei Beendigung der Leistungsvereinbarung kann der Verantwortliche seine Daten nach Maßgabe von Ziffer 11.8 und 11.9 der AGB exportieren. Danach, spätestens 30 Kalendertage nach Vertragsende, oder früher auf Aufforderung des Verantwortlichen löscht der Auftragsverarbeiter sämtliche im Zusammenhang mit dem Auftragsverhältnis stehenden Daten einschließlich Kopien datenschutzgerecht, soweit keine gesetzliche Pflicht zur Speicherung besteht. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll wird dem Verantwortlichen auf Anforderung zur Verfügung gestellt.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen auch über das Vertragsende hinaus aufbewahren oder sie dem Verantwortlichen zu seiner Entlastung bei Vertragsende übergeben. Nach Ende der Aufbewahrungsfrist gilt Absatz 2.

(4) Für die Löschung gilt ein dem Stand der Technik angemessenes Löschkonzept, das auch in Backup-, Snapshot- und Archivsystemen gespeicherte Daten berücksichtigt. Daten in Sicherungskopien dürfen bis zum Ablauf der intern dokumentierten Rotationsfristen gespeichert bleiben und werden danach im Rahmen der regelmäßigen Lösch- oder Überschreibungsverfahren entfernt oder irreversibel unkenntlich gemacht. Die Absicherung solcher Sicherungskopien richtet sich nach Anhang A.

(5) Beendet der Verantwortliche die Inanspruchnahme der Leistungen, unterstützt der Auftragsverarbeiter ihn nach Maßgabe von Ziffer 11.8 der AGB bei der Herauslösung und Übernahme der Daten sowie wesentlicher zugehöriger digitaler Bestandteile in strukturierten, gängigen und maschinenlesbaren Formaten. Die Unterstützung umfasst auch Informationen zu Speicher-, Sicherungs- und Exportpfaden, soweit dies für einen geordneten Wechsel erforderlich ist. Weitergehende gesetzliche Anforderungen, insbesondere nach der Verordnung (EU) 2023/2854 (Data Act), bleiben unberührt.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

§ 9 Weitere Auftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen. Die bei Vertragsschluss eingesetzten weiteren Auftragsverarbeiter sind in Anhang B aufgeführt; mit deren Einsatz ist der Verantwortliche einverstanden. Infrastrukturanbieter, die der Verantwortliche bei der Buchung einer Ressource selbst auswählt, gelten mit dieser Auswahl als genehmigt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Kalendertage vor Wirksamwerden in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters. Die Information enthält, soweit einschlägig, die Bezeichnung des weiteren Auftragsverarbeiters, die betroffene Leistung, die betroffenen Datenkategorien, den Standort bzw. die Region der Verarbeitung, einen etwaigen Drittlandbezug sowie die vorgesehenen Garantien. Die Hinzufügung neuer Infrastrukturanbieter, die nur für neu buchbare Regionen eingesetzt werden, kann durch Aktualisierung von Anhang B erfolgen, da sie erst mit der Auswahl durch den Verantwortlichen eingesetzt werden.

(3) Der Verantwortliche kann einer Änderung nach Absatz 2 Satz 1 innerhalb von 14 Kalendertagen nach Zugang der Information aus sachlich gerechtfertigten datenschutzrechtlichen Gründen in Textform widersprechen. Im Fall eines berechtigten Widerspruchs prüfen die Vertragsparteien unverzüglich eine zumutbare Alternative. Steht keine zur Verfügung, kann der Verantwortliche die betroffenen Services ohne Einhaltung einer Frist zum Zeitpunkt des Wirksamwerdens der Änderung kündigen; weitere Rechte aus der Leistungsvereinbarung bleiben unberührt.

(4) In dringenden Ausnahmefällen, insbesondere zur Aufrechterhaltung oder Wiederherstellung der Sicherheit oder Verfügbarkeit der Leistungen, darf der Auftragsverarbeiter einen weiteren Auftragsverarbeiter mit verkürzter Frist einsetzen, sofern er den Verantwortlichen unverzüglich informiert und die übrigen Voraussetzungen dieses Paragrafen einhält.

(5) Nicht als weitere Auftragsverarbeiter gelten Dritte, deren Leistungen der Auftragsverarbeiter als reine Nebenleistung zur Unterstützung seiner allgemeinen Geschäftstätigkeit in Anspruch nimmt (z. B. Telekommunikationsleistungen, Reinigung), sofern sie nicht mit spezifischen Verarbeitungstätigkeiten im Zusammenhang mit diesem Auftrag betraut werden. Der Auftragsverarbeiter stellt auch in diesen Fällen durch angemessene vertragliche, technische und organisatorische Maßnahmen den Schutz der Daten sicher. Ebenfalls keine weiteren Auftragsverarbeiter sind Anbieter von Integrationen, die der Verantwortliche selbst mit der Plattform verbindet, etwa GitHub, GitLab oder ein eigener Identitätsanbieter. Für die Verarbeitung bei diesen Anbietern gilt das Vertragsverhältnis zwischen dem Verantwortlichen und dem jeweiligen Anbieter.

(6) Der Auftragsverarbeiter gestaltet seine Verträge mit weiteren Auftragsverarbeitern so, dass ihnen dieselben Datenschutzpflichten auferlegt werden, die in dieser Vereinbarung festgelegt sind, insbesondere hinsichtlich geeigneter technischer und organisatorischer Maßnahmen. Der Verantwortliche kann auf Anforderung in Textform Auskunft über den wesentlichen Inhalt dieser Verträge und die Umsetzung der datenschutzrelevanten Pflichten erhalten, soweit hierdurch keine Betriebs- oder Geschäftsgeheimnisse oder Rechte Dritter unangemessen beeinträchtigt werden.

(7) Kommt ein weiterer Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung dieser Pflichten. Er hat in diesem Fall auf Verlangen des Verantwortlichen die Beauftragung des weiteren Auftragsverarbeiters ganz oder teilweise zu beenden, wenn und soweit dies nicht unverhältnismäßig ist.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

§ 10 Datenschutzkontrolle durch Aufsichtsbehörden

(1) Der Auftragsverarbeiter gewährt der oder dem Datenschutzbeauftragten des Verantwortlichen sowie der für den Verantwortlichen zuständigen Aufsichtsbehörde zur Erfüllung ihrer im Zusammenhang mit diesem Auftrag gesetzlich übertragenen Aufgaben im erforderlichen Umfang Zugang zu den üblichen Geschäftszeiten. Betretung, Einsicht und Befragung beschränken sich auf das zur Überprüfung dieses Auftragsverhältnisses erforderliche Maß, sind vertraulich zu behandeln und dürfen die Interessen anderer Kunden sowie Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters nicht unangemessen beeinträchtigen; Bereiche ohne Bezug zur Auftragserfüllung bleiben ausgenommen. Soweit gesetzlich zulässig, nutzen die Parteien hierfür vorrangig die Verfahren nach § 6 Abs. 3 bis 6.

(2) Einsicht in Unterlagen, die durch Berufsgeheimnisse oder vergleichbare gesetzliche Geheimhaltungsregeln geschützt sind, erfolgt nur im unvermeidbar erforderlichen Umfang. Die Mitarbeiter des Auftragsverarbeiters werden angewiesen, im Rahmen des Erforderlichen und rechtlich Zulässigen mitzuwirken und Fragen wahrheitsgemäß zu beantworten. Verschwiegenheits- und Zeugnisverweigerungsrechte bleiben unberührt.

(3) Über Anfragen und Maßnahmen von Aufsichtsbehörden, die diesen Auftrag sowie Daten oder Systeme anderer Kunden gemeinsam berühren können, stimmen sich die Parteien unverzüglich ab, soweit dem keine zwingenden gesetzlichen Vorgaben entgegenstehen.

§ 11 Schlussbestimmungen

(1) Bei Widersprüchen zwischen dieser Vereinbarung und der Leistungsvereinbarung geht diese Vereinbarung in Fragen des Datenschutzes vor.

(2) Für die Haftung der Vertragsparteien untereinander gelten die Regelungen der Leistungsvereinbarung, insbesondere Ziffer 13 der AGB. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

(3) Der Auftragsverarbeiter kann diese Vereinbarung einschließlich ihrer Anhänge nach dem Verfahren der Ziffer 16 der AGB ändern, soweit die Änderung das Schutzniveau nicht verringert. Änderungen von Anhang B richten sich nach § 9. Im Übrigen bedürfen Änderungen und Ergänzungen der Textform und des ausdrücklichen Hinweises, dass es sich um eine Änderung dieser Vereinbarung handelt.

(4) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, bleibt die Wirksamkeit der übrigen Regelungen unberührt. An die Stelle der unwirksamen oder undurchführbaren Regelung treten die gesetzlichen Vorschriften.

Abschluss

(1) Diese Vereinbarung ist einschließlich ihrer Anhänge Bestandteil des Plattformvertrags (Ziffer 14.1 der AGB) und wird mit dessen Abschluss verbindlich vereinbart. Einer gesonderten Unterzeichnung bedarf es nicht (Art. 28 Abs. 9 DSGVO).

(2) Soweit die Plattform dies vorsieht, kann der Verantwortliche dort kundenspezifische Angaben zur Verarbeitung hinterlegen und aktualisieren, insbesondere zu Datenkategorien und Kategorien betroffener Personen. Diese Angaben konkretisieren den Auftrag innerhalb des vereinbarten Leistungsumfangs und werden Bestandteil dieser Vereinbarung. Sie erweitern weder den Leistungsumfang noch die technischen und organisatorischen Maßnahmen nach Anhang A. Der Auftragsverarbeiter dokumentiert die Angaben und ihre Änderungen mit Zeitpunkt, Organisation und handelndem Account.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

(3) Die jeweils geltende Fassung dieser Vereinbarung einschließlich etwaiger kundenspezifischer Angaben stellt der Auftragsverarbeiter dem Verantwortlichen zum Download bereit. Wünscht der Verantwortliche ein unterzeichnetes Exemplar oder wird eine abweichende Vereinbarung in einem Enterprise-Vertrag getroffen, gilt die folgende Unterzeichnung für die Vereinbarung einschließlich aller Anhänge.

Verantwortlicher	**Auftragsverarbeiter**
Firma:	Loopback GmbH
Ort, Datum:	Schwalbach,
Name, Funktion:	Jonathan Bouillon, Geschäftsführer
Unterschrift:	Unterschrift:

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

Anhang A – Technisch-organisatorische Maßnahmen

1. Grundsatz

Die Vertragsparteien setzen geeignete technische und organisatorische Maßnahmen so um, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und die Rechte und Freiheiten der betroffenen Personen angemessen geschützt sind.

2. Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter gestaltet seine interne Organisation so, dass sie den Anforderungen des Datenschutzes und der Informationssicherheit gerecht wird. Er trifft insbesondere solche Maßnahmen, die unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten betroffener Personen geeignet und angemessen sind.

3. Geltungsbereich der Maßnahmen

Die Maßnahmen gelten für die vom Auftragsverarbeiter betriebenen oder verantworteten Systeme und Verarbeitungsumgebungen. Für Rechenzentren und physische Infrastruktur der Infrastrukturanbieter gelten deren Maßnahmen, die der Auftragsverarbeiter bei Auswahl und Überprüfung der Anbieter berücksichtigt, insbesondere anhand von Zertifizierungen wie ISO 27001 oder BSI C5. Für kundeneigene Infrastruktur und für Konfigurationen, die der Verantwortliche selbst vornimmt, gelten die Maßnahmen nur, soweit sie im Verantwortungs- und Einflussbereich des Auftragsverarbeiters liegen.

4. Einzelmaßnahmen nach Art. 32 DSGVO

Nr.	Maßnahme	Umsetzung
1	**Zutrittskontrolle**: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen zu verwehren.	Physische Standorte und Betriebsbereiche werden durch angemessene organisatorische und technische Zutrittsschutzmaßnahmen gesichert. Zutritte zu sicherheitsrelevanten Bereichen erfolgen nur für berechtigte Personen, werden kontrolliert und, soweit vorgesehen, protokolliert. Besucher- und Dienstleisterzugänge unterliegen einem geregelten Freigabe-, Identifikations- und Begleitprozess. Für Rechenzentren der Infrastrukturanbieter gilt Ziffer 3.
2	**Zugangskontrolle**: Die Nutzung von Datenverarbeitungssystemen durch Unbefugte ist zu verhindern.	Zugänge zu Code-Repositories, Dokumentation, Management-Oberflächen, administrativen Systemen und Infrastruktur erfolgen über föderierte oder zentral verwaltete Authentifizierung, insbesondere OIDC, OAuth oder vergleichbare Verfahren. Mehrfaktor-Authentifizierung wird für privilegierte Zugänge und, soweit risikoadäquat, für weitere schutzbedürftige Zugänge eingesetzt. Authentisierungsmerkmale werden individuell vergeben; gemeinsame Konten werden vermieden oder besonders kontrolliert. Zugang besteht nur für berechtigte Personen mit dokumentierter Rollen- und Aufgabenbindung. Privilegierte Zugänge werden besonders geschützt und nur im erforderlichen Umfang gewährt.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

Nr.	Maßnahme	Umsetzung
3	**Zugriffskontrolle**: Berechtigte dürfen nur auf die ihrer Berechtigung unterliegenden Daten zugreifen; Daten dürfen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.	Berechtigungen werden dokumentiert, nach Rollen und Verantwortlichkeiten vergeben und bei Aufgabenwechsel oder Ausscheiden entzogen oder angepasst. Zugriffe erfolgen nur im zur Leistungserbringung erforderlichen Umfang nach dem Least-Privilege-Prinzip. Der Zugriff erfolgt rollenbasiert; in der mandantenfähigen Plattform zusätzlich entlang von Organisations-, Projekt-, Namespace- oder vergleichbaren Abgrenzungen. Zugriffsrechte und administrative Rollen werden regelmäßig überprüft. Administrative Zugriffe und sicherheitsrelevante Änderungen werden protokolliert. Systeme im Verantwortungsbereich des Auftragsverarbeiters werden fortlaufend mit sicherheitsrelevanten Updates versorgt.
4	**Weitergabekontrolle**: Daten dürfen bei Übertragung, Transport oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden; Übermittlungsstellen müssen feststellbar sein.	Daten werden bei der Übertragung kryptographisch geschützt; für öffentlich erreichbare Transportwege wird in der Regel TLS 1.3 oder ein vergleichbares Niveau eingesetzt. Verbindungen zwischen Clustern und zu angebundener Infrastruktur werden verschlüsselt (z. B. WireGuard). Ruhende Daten in verwalteten Speicher- und Backup-Systemen werden, soweit vorgesehen, verschlüsselt. Schlüssel und Secrets werden über dokumentierte Key-Management-Prozesse verwaltet. Übermittlungen an Dritte oder in Drittländer erfolgen nur im Rahmen dieser Vereinbarung, dokumentierter Weisungen und der erforderlichen Garantien.
5	**Eingabekontrolle**: Es muss nachträglich feststellbar sein, ob und von wem Daten eingegeben, verändert oder entfernt worden sind.	Sicherheits-, administrations- und änderungsrelevante Aktionen in der Plattform werden über Audit- und Systemprotokolle nachvollziehbar erfasst, insbesondere API-, Administrations- und Änderungsprotokolle. Protokolle werden vor unbefugter Änderung geschützt und in einem geregelten Verfahren oder anlassbezogen ausgewertet. Anmelde- und Sicherheitsereignisse werden 90 Tage, Audit-Protokolle der Organisation 12 Monate aufbewahrt, soweit keine abweichenden Vorgaben bestehen.
6	**Auftragskontrolle**: Daten dürfen nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden.	Verarbeitungen erfolgen nur auf Grundlage der Leistungsvereinbarung, dieser Vereinbarung und dokumentierter Weisungen. Mitarbeiter sind auf Vertraulichkeit, Zweckbindung und weisungsgebundenen Umgang verpflichtet und werden regelmäßig sensibilisiert. Support-, Wartungs-, Fernwartungs- und administrative Zugriffe unterliegen dokumentierten Prozessen, rollenbezogenen Freigaben und nachvollziehbarer Verantwortungszuordnung. Datenschutz und Informationssicherheit sind in die betrieblichen Prozesse eingebunden. Weitere Auftragsverarbeiter werden nur nach dokumentierter Auswahl, Einbindung und Kontrolle eingesetzt.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

Nr.	Maßnahme	Umsetzung
7	**Verfügbarkeitskontrolle**: Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.	Für die vom Auftragsverarbeiter betriebenen Komponenten bestehen dokumentierte Backup-, Restore- und Wiederherstellungsverfahren nach Ziffer 7 des Leistungsanhangs; die Sicherung von Kundeninhalten obliegt dem Verantwortlichen, soweit nicht anders vereinbart. Sicherungen werden logisch oder räumlich getrennt gespeichert und gegen unbefugten Zugriff geschützt. Monitoring, Alarmierung und Maßnahmen zur Erkennung von Störungen und Angriffen werden eingesetzt. Je nach Einsatzszenario werden Redundanzen, abgesicherte Speicherverfahren, Strom- und Netzabsicherung sowie DDoS-Schutz verwendet. Für Vorfälle bestehen geregelte Eskalations- und Wiederanlaufverfahren; Wiederherstellungstests erfolgen risikoadäquat und dokumentiert.
8	**Trennungskontrolle**: Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.	Daten werden physisch oder logisch getrennt verarbeitet und gespeichert, auch in Sicherungskopien, soweit vorgesehen. In der mandantenfähigen Plattform erfolgt die Trennung über Organisationen, Projekte, Cluster, Namespaces oder vergleichbare Abgrenzungen, rollenbasierte Zugriffstrennung und Netzwerksegmentierung. Test-, Staging- und Produktionsumgebungen werden getrennt betrieben oder logisch abgegrenzt. Logging-, Backup- und Betriebsprozesse nutzen getrennte oder logisch abgegrenzte Verarbeitungswege, soweit möglich und angemessen.

5. Ergänzende cloud- und plattformspezifische Kontrollen

Vulnerability Management und Patching. Der Auftragsverarbeiter setzt Verfahren zur Identifikation, Bewertung und Behandlung sicherheitsrelevanter Schwachstellen ein, insbesondere sicherheitsbezogene Updates, Patches, Wartungs- und Änderungsprozesse sowie die risikoorientierte Behandlung kritischer Befunde.

Netzwerksicherheit und Segmentierung. Netzwerkzugänge und Kommunikationsbeziehungen werden nach dem Grundsatz der erforderlichen Freigabe ausgestaltet, insbesondere durch Segmentierung, restriktive Netzwerkregeln, abgesicherte Ingress- und Egress-Pfade sowie Maßnahmen gegen netzbasierte Angriffe.

Incident Response. Für sicherheits- und betriebsrelevante Vorfälle bestehen dokumentierte Reaktionsverfahren für Erkennung, Bewertung, Eingrenzung, Behebung, Wiederherstellung und Nachbereitung sowie geregelte Kommunikations- und Eskalationswege.

Remote Work Controls. Zugriffe aus Homeoffice oder anderen externen Arbeitsumgebungen erfolgen nur über verwaltete oder angemessen gehärtete Endgeräte, mit Verschlüsselung, starker Authentifizierung und abgesicherten Fernzugängen sowie unter Vermeidung unkontrollierter lokaler Datenspeicherung. Administrative Zugriffe bleiben nachvollziehbar.

Zugangsdaten, Geheimnisse und Konfigurationsdaten. Zugangsdaten und sonstige sicherheitsrelevante Informationen, insbesondere Passwörter, Tokens, Schlüsselmaterial, kubeconfig-Dateien und Zertifikate, stellt der Auftragsverarbeiter dem Verantwortlichen über die authentifizierte Plattform oder API bereit. Andere Übermittlungswege werden nur genutzt, wenn sie verschlüsselt, zugriffsbeschränkt und zeitlich begrenzt sind; Freigabeinformationen werden dabei getrennt übermittelt.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

6. Regelmäßige Überprüfung und Nachweisführung

Die Wirksamkeit der Maßnahmen wird in angemessenen, risikoorientierten Intervallen überprüft, insbesondere durch Reviews von Berechtigungen, Protokollen, Schwachstellenbehandlungen und Wiederherstellungsverfahren. Der Auftragsverarbeiter dokumentiert wesentliche Ergebnisse, etwa durch Testate, Berichte unabhängiger Stellen, Auszüge aus Sicherheits- oder Auditdokumentationen, Protokolle zu Restore-Tests oder Nachweise zu Access Reviews. Nachweise werden dem Verantwortlichen im Rahmen von § 6 in geeigneter Form zur Verfügung gestellt, soweit keine Betriebs- oder Geschäftsgeheimnisse, Sicherheitsinteressen oder Rechte Dritter unangemessen beeinträchtigt werden.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

Anhang B – Weitere Auftragsverarbeiter

B.1 Für alle Services

Firma	Leistung	Standort	Garantien bei Drittlandbezug
ayedo Cloud Solutions GmbH, Gottlieb-Daimler-Straße 1-7, 66773 Schwalbach	interne Plattform- und Betriebsinfrastruktur, Basisdienste	Deutschland	–
SP4RK UG (haftungsbeschränkt), Gottlieb-Daimler-Straße 1-7, 66773 Schwalbach	E-Mail, insbesondere Support-Korrespondenz und System-E-Mails	Deutschland	–
Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA	Proxy und DNS für Website, Plattform und API	EU / USA	EU-US Data Privacy Framework, Standardvertragsklauseln
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Rechenzentrum und Infrastruktur für Plattform, API und Steuerungskomponenten	Deutschland (Falkenstein, Nürnberg)	–

B.2 Infrastrukturanbieter für vom Verantwortlichen gewählte Regionen

Diese Anbieter werden nur eingesetzt, wenn der Verantwortliche bei der Buchung einer Ressource den jeweiligen Anbieter und die Region auswählt (§ 9 Abs. 1 Satz 3). Welche Regionen für welchen Service verfügbar sind, zeigt die Plattform bei der Buchung an. Derzeit liegen alle Regionen in der Europäischen Union.

Firma	Leistung	Länder der Regionen	Garantien bei Drittlandbezug
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Compute, Block-Storage, Object Storage, Load Balancer, Netzwerk	Deutschland, Finnland	–
IONOS Cloud GmbH, Elgendorfer Str. 57, 56410 Montabaur	Compute, Block-Storage, Object Storage, Load Balancer, Netzwerk	Deutschland, Frankreich, Spanien	–

B.3 Für einzelne Services

Firma	Service	Leistung	Standort
OpusDNS GmbH, Franz-Mayer-Straße 1, 93053 Regensburg	DNS und Domains	Nameserver, Verwaltung von DNS-Zonen, Domainregistrierung	Deutschland

B.4 Zur Information: Dienstleister für eigene Zwecke des Auftragsverarbeiters

Die folgenden Dienstleister verarbeiten keine Daten im Auftrag des Verantwortlichen, sondern Daten, für die der Auftragsverarbeiter selbst verantwortlich ist, etwa Kontakt- und Rechnungsdaten der Ansprechpartner des Verantwortlichen (§ 1 Abs. 2). Sie sind hier nur zur Transparenz aufgeführt; Näheres regelt die Datenschutzerklärung.

Firma	Leistung	Standort
everii Switzerland GmbH, In der Weid 15, 8122 Binz, Schweiz	Kundenverwaltung und Buchhaltung (MOCO)	Schweiz

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

Firma	Leistung	Standort
CFTools Software GmbH, Benzstraße 13, 84030 Landshut	Rechnungsstellung und Buchhaltung (billDynamic)	Deutschland
Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland	Zahlungsabwicklung	EU / USA
Peters & Müller Steuerberaterkanzlei, Stiftstraße 16, 66740 Saarlouis	Steuerberatung (Berufsgeheimnisträger)	Deutschland

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud

Anhang C – Weisungsberechtigte und Weisungswege

C.1 Verantwortlicher

Wer eine Organisation anlegt, erhält darin die Rolle mit sämtlichen Berechtigungen („Root“). Root kann anderen Mitgliedern Rollen mit fein abgestuften Berechtigungen zuweisen und ihnen, soweit so konfiguriert, auch die Vergabe von Rollen erlauben.

Weisungsberechtigt ist jedes Mitglied der Organisation des Verantwortlichen im Umfang der ihm in der Plattform eingeräumten Berechtigungen. Weisungen, die über die Funktionen der Plattform hinausgehen, können Mitglieder mit der Rolle Root und zur Vertretung des Verantwortlichen berechtigte Personen erteilen. In Enterprise-Verträgen können weisungsberechtigte Personen namentlich benannt werden.

C.2 Auftragsverarbeiter

Weisungen nimmt der Auftragsverarbeiter entgegen über

- die Funktionen der Plattform und der API,
- E-Mail an support@loopback.cloud,
- das Ticketsystem in der Plattform, sobald verfügbar.

Weisungsempfänger beim Auftragsverarbeiter ist die Geschäftsführung, derzeit Jonathan Bouillon, sowie die von ihr benannten Mitarbeiter des Supports.

C.3 Informationswege

Mitteilungen des Auftragsverarbeiters an den Verantwortlichen, insbesondere nach § 7 und § 9, erfolgen per E-Mail an die in der Organisation hinterlegte Adresse und, soweit möglich, zusätzlich in der Plattform. Der Verantwortliche hält diese Adresse aktuell.

Loopback GmbH
Registergericht: Saarbrücken
Registernummer: HRB 111974

Gottlieb-Daimler-Straße 1-7
66773 Schwalbach
hello@loopback.cloud | loopback.cloud