Anlage 3
Auftragsverarbeitungsvereinbarung gem. Art. 28 DSGVO („AVV“)

zwischen

Leadtime Labs GmbH, Yorckstr. 22, 93049 Regensburg

- Auftragsverarbeiter, im Folgenden: Auftragnehmer -

und

- Verantwortlicher, im Folgenden: Auftraggeber -

- im Folgenden auch gemeinsam „Parteien“ und einzeln „Partei“ genannt -

Präambel

Diese Vereinbarung legt die Rechte und Pflichten des Auftragnehmers und des Auftraggebers im Rahmen der Verarbeitung von personenbezogenen Daten im Auftrag gemäß Art. 28 der EU-Datenschutzgrundverordnung („DSGVO“) fest. Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Der Gegenstand der Verarbeitung ergibt sich aus dem Vertrag über die Erbringung von IT-Dienstleistungen („IT-Projektvertrag“), auf den im Folgenden verwiesen wird (nachfolgend „Hauptvertrag“ genannt).

(2) Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

(3) Soweit die Laufzeit des Hauptvertrags beendet sein sollte, gilt diese Vereinbarung unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

§ 2 Art der Daten und Zweck der Verarbeitung

(1) Der Auftragnehmer erbringt für den Auftraggeber die IT-Dienstleistungen gemäß des Hauptvertrags, insbesondere folgende Leistungen: Betrieb eines Leadtime Workspace“. Darüber hinaus erbringt der Anbieter Wartungs- und Supportleistungen für den Auftraggeber, wodurch die Möglichkeit des Zugriffs auf die nachstehend genannten Arten personenbezogener Daten besteht.

(2) Gegenstand der Verarbeitung personenbezogener Daten können dabei die folgenden Datenarten/-kategorien sein:

- allgemeine Personendaten (Name, Titel, akademischer Abschluss, Geburtsdatum)
- Kommunikationsdaten (Anschrift, Telefonnummer, E-Mail)
- Zahlungsdaten (Bankverbindung)
- Gesundheitsdaten (Krankheitstage von Mitarbeitern, ärztliche Atteste)
- Soziale Daten (Krankenversicherungsnummer, Rentenversicherung, Sozialversicherungsnummer, Einkommensteuerklasse)

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

- Beschäftigte des Auftraggebers
- Freelancer
- Kunden und avisierte Kunden des Auftraggebers.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer versichert, dass ihm die einschlägigen, geltenden Datenschutzvorschriften bekannt sind und er jederzeit die Grundsätze zur ordnungsgemäßen Verarbeitung personenbezogener Daten beachtet. Diese Vereinbarung entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten grundsätzlich nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn, er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Die anfänglichen Weisungen des Auftraggebers werden durch diese

Vereinbarung und den Hauptvertrag festgelegt. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Meinung ist, eine Weisung verstoße gegen geltende Datenschutzvorschriften.

(3) Der Auftragnehmer wird die Daten für keine anderen als die festgelegten Zwecke verwenden.

(4) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung der Daten die Vertraulichkeit zu wahren und setzt bei der Erbringung seiner Leistungen nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

(5) Die Parteien arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diese Vereinbarung und die Verarbeitung der Daten des Auftraggebers beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten nach dieser Vereinbarung beim Auftragnehmer ermittelt.

(7) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technisch-organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen sichergestellt ist.

(8) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Kenntnisnahme an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere gem. Art. 33, 34 DSGVO nachkommen kann. Er wird über den gesamten Vorgang eine Dokumentation erstellen, die er dem Auftraggeber auf Nachfrage zur Kenntnisnahme und für weitere Maßnahmen übermittelt.

(9) Der Auftragnehmer verpflichtet sich, den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen zur Verfügung zu stellen.

(10) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, wird der Auftragnehmer den Auftraggeber auf dessen Kosten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen. Dies gilt gleichermaßen für eine ggf. bestehende Pflicht zur Konsultation der zuständigen Datenschutz- Aufsichtsbehörde. Die Parteien werden sich über die Modalitäten und Konditionen im Einzelfall schriftlich oder in Textform verständigen.

§ 4 Technisch-organisatorische Maßnahmen („TOMs“)

(1) Der Auftragnehmer verpflichtet sich, in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorischen Maßnahmen gem. Art. 32 DSGVO zum Schutze der personenbezogenen Daten zu ergreifen, die im Auftrag des Auftraggebers verarbeitet werden. Die Dokumentation der technisch-organisatorischen Maßnahmen wird zum Zeitpunkt des Vertragsschlusses in Anhang 1 verbindlich zwischen den Parteien festgelegt.

(2) Die in Anhang 1 dargestellten technisch-organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, entsprechend angepasste Maßnahmen in Zukunft umzusetzen, wobei das Sicherheitsniveau der vorliegend festgelegten Maßnahmen nicht unterschritten werden darf. Der Auftragnehmer wird sämtliche Änderungen dokumentieren und den Auftraggeber über wesentliche Änderungen unverzüglich in Kenntnis setzen.

§ 5 Umgang mit Rechten der betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anfragen seitens betroffener Personen in Bezug auf deren Datenschutzrechte.

(2) Der Auftragnehmer wird Daten, die im Auftrag verarbeitet werden, nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers beauskunften, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich bei Ausübung ihrer Datenschutzrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

§ 6 Einsatz von Unterauftragnehmern

(1) Der Auftragnehmer ist berechtigt, Unterauftragnehmer als weitere Auftragsverarbeiter im Rahmen der Verarbeitung personenbezogener Daten einzusetzen. Der Auftraggeber gestattet den Einsatz der in Anhang 2 aufgeführten Unterauftragnehmer.

(2) Die Auslagerung auf weitere Unterauftragnehmer sowie jeder Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmer sind zulässig, soweit:

(a) der Auftragnehmer eine solche Auslagerung bzw. den Wechsel dem Auftraggeber mit einer Frist von 4 Wochen vorab schriftlich oder in Textform anzeigt und

(b) der Auftraggeber nicht innerhalb von 2 Wochen nach Erhalt der Anzeige gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

(c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 - 4 DSGVO mit dem Unterauftragnehmer besteht.

(3) Im Falle eines Einspruchs des Auftraggebers gegen eine solche Auslagerung bzw. gegen den Wechsel eines Unterauftragnehmers hat der Auftragnehmer das Recht zur außerordentlichen Kündigung dieser Vereinbarung und des Hauptvertrags aus wichtigem Grund.

(4) Der Auftragnehmer wird die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer unter Berücksichtigung des jeweiligen Risikos vor Beginn der Verarbeitung personenbezogener Daten und sodann regelmäßig kontrollieren. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung.

(5) Sofern der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR erbringt, wird der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch geeignete Maßnahmen, insbesondere durch angemessene Datenschutzgarantien, sicherstellen.

(6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers schriftlich oder in Textform.

(7) Im Sinne der vorstehenden Regelungen handelt es sich bei Unterauftragsverhältnissen um solche Leistungen, die sich unmittelbar auf die hauptvertragliche Leistungserbringung beziehen. Hierunter fallen grundsätzlich nicht Nebenleistungen wie z.B. Telekommunikationsdienstleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach dieser Vereinbarung stehen.

§ 7 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Beurteilung der Zulässigkeit der Auftragsverarbeitung sowie hinsichtlich der Wahrung der Betroffenenrechte allein verantwortlich.

(2) Der Auftraggeber hat ein umfassendes Weisungsrecht hinsichtlich der Verarbeitung personenbezogener Daten im Auftrag. Hierzu benennen die Parteien die nachfolgend genannten Personen, die jeweils ausschließlich zur Erteilung und zur Annahme von Weisungen befugt sind:

Befugte Personen bei	Auftraggeber	Auftragnehmer
Name, Vorname	Ebner, Lukas	
E-Mail-Adresse	lukas@leadtime.de	
Telefonnummer	+49 941 463 900 42	

(3) Eine Änderung von befugten Personen und/oder deren Kontaktdaten ist der jeweils anderen Partei unverzüglich schriftlich oder in Textform mitzuteilen.

(4) Der Auftraggeber ist verpflichtet, alle Aufträge, Teilaufträge oder Weisungen in dokumentierter Form, d.h. mindestens in Textform, zu erteilen. Nur in dringenden Ausnahmen dürfen Weisungen mündlich erteilt werden; solche Weisungen hat der Auftraggeber unverzüglich und in entsprechender Weise dokumentiert zu bestätigen.

(5) Der Auftraggeber verpflichtet sich, den Auftragnehmer unverzüglich zu informieren, sofern und soweit er Fehler oder Unregelmäßigkeiten im Rahmen der Auftragsverarbeitung feststellt.

(6) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften zum Datenschutz sowie die vertragli-

chen Vereinbarungen, insbesondere die vollständige Umsetzung der festgelegten technisch-organisatorischen Maßnahmen und deren Wirksamkeit, beim Auftragnehmer in angemessenem Umfang selbst oder durch einen im Einzelfall zu benennenden Prüfer zu kontrollieren. Kontrollen sind insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme möglich. Der Auftragnehmer ist verpflichtet, notwendige Auskünfte zu erteilen und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

§ 8 Datenverarbeitung außerhalb EU/EWR

(1) Sofern eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation erforderlich sein sollte, wird der Auftragnehmer die Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel 5 der DSGVO sicherstellen.

(2) Der Auftraggeber gestattet die Datenübermittlung in ein Drittland an die in Anhang 2 genannten Empfänger. Aus dem Anhang ergeben sich die vom Auftraggeber genehmigten Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung.

(3) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung der Regelungen nach Kapitel 5 der DSGVO allein verantwortlich.

§ 9 Beendigung der Verarbeitung im Auftrag

(1) Nach Beendigung der Zusammenarbeit wird der Auftragnehmer auf Verlangen des Auftraggebers die personenbezogenen Daten gemäß der vereinbarten Aufbewahrungsfrist an den Auftraggeber übergeben und anschließend von den Servern löschen. Dieses Verlangen hat der Kunde binnen einem (1) Monat nach Beendigung der Zusammenarbeit auszuüben. Die Löschung erfolgt dergestalt, dass eine Wiederherstellung mit vertretbarem Aufwand unmöglich ist.

(2) Der Auftragnehmer wird die Löschung auch gegenüber seinen Unterauftragnehmern sicherstellen, soweit dies vertraglich möglich und rechtlich zulässig ist.

(3) Der Auftragnehmer ist zum Nachweis der ordnungsgemäßen Löschung verpflichtet und wird diesen dem Auftraggeber entsprechend vorlegen. Der Auftragnehmer ist berechtigt, Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, entsprechend den jeweiligen Aufbewahrungsfristen auch über die Laufzeit der Vereinbarung hinaus aufzubewahren.

§ 10 Schlussbestimmungen

(1) Diese Vereinbarung gilt vorrangig, auch soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, es sei denn, die Parteien haben ausdrücklich etwas anderes vereinbart.

(2) Diese Vereinbarung ersetzt damit alle mündlichen oder schriftlich getroffenen Abreden, die zuvor zwischen den Parteien hinsichtlich des Gegenstands der Verarbeitung getroffen wurden.

(3) Darüber hinaus gehende mündliche oder schriftliche Nebenabreden zu dieser Vereinbarung wurden nicht getroffen.

(4) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform, soweit nicht eine Individualvereinbarung getroffen wurde. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.

(5) Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der Vereinbarung sowie der verbleibenden Bestimmungen im Übrigen nicht berührt. Die Parteien werden sich bemühen, eine wirksame und durchführbare Bestimmung zu vereinbaren, die dem verfolgten wirtschaftlichen Zweck der unwirksamen oder undurchführbaren Bestimmung am nächsten kommt. Dies gilt gleichermaßen im Falle einer Regelungslücke.

(6) Die nachstehend aufgeführten Anhänge zu dieser Vereinbarung sind integraler und wesentlicher Vertragsbestandteil:

Anlage 3 – Anhang 1
Technisch-organisatorische Maßnahmen („TOMs“) beim Auftragnehmer

Nachfolgend aufgeführte technisch-organisatorische Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit sind derzeit beim Auftragnehmer und/oder seinen Unterauftragnehmern vorhanden:

Nr	Gebiet	Beschreibung
0	**Organisation**	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus der DSGVO eingesetzt.
	Namen und Kontaktdaten des Datenschutzbeauftragten	Wojtek Dragon Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg anfrage@projekt29.de
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter und fachbezogene Webschulungen.
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Im Rahmen des internen Verfahrens-verzeichnisses sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach DS-GVO nachgewiesen. Eventuell notwendige Vorabkontrollen werden schon im Planungsstadium integriert.
1	**Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**	
1.1	**Zutrittskontrolle**	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Das Gebäude ist mit einer Sicherheits-Schließanlage ausgerüstet.
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Die Räume werden ebenfalls durch das Sicherheitsschließsystem gesichert.
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Die Rechenzentren von DigitalOcean befinden sich in unauffälligen Gebäuden, die physisch gebaut, verwaltet und rund um die Uhr überwacht werden, um Daten und Services vor unbefugtem Zugriff sowie vor Umweltbedrohungen zu schützen. Alle Rechenzentren sind von einem Zaun umgeben und der Zugang ist durch ausweisgesteuerte Tore beschränkt.
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.
1.2	**Zugangskontrolle**	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Benutzerzugänge werden nur sehr selektiv und nur nach Genehmigung durch die Geschäftsführung vergeben. Zugriff auf kaufmännische Dokumente und Kommunikationsinformationen sind durch starke Passwörter geschützt
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Alle Rechte werden unter Wahrung des Minimalprinzips vergeben und nur bei Bedarf erweitert. Bei Austritt werden stets alle Zugänge entzogen.
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Die Entscheidungen zur Rechtevergabe halten sich streng an die entsprechenden Vorgaben, Datenvermeidung und Datensparsamkeit.
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Der Einsatz von Heimarbeitsplätzen ist mittels einer Home-Office Richtlinie abgesichert. Die Mitarbeiter sind aufgefordert, zuhause dieselben Maßnahmen zu pflegen wie im Betrieb.
1.2	**Zugriffskontrolle**	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Die Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Die strengen Systemvoreinstellungen zwingen zu einer hohen Passwortkomplexität. Passwörter werden nicht im Klartext gespeichert oder notiert.
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Die Vorgaben und Empfehlungen des BSI dienen als Vorbild für die o.g. Systemeinstellungen

	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Schulung und Sensibilisierung der Mitarbeiter. Einweisungen und regelmäßige Schulungen zu den verwendeten Geräten
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Siehe auch Punkt Vergabe von Benutzerzugängen Punkt 1.2; die IT-Abteilung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Jeder bekommt minimale Rechte zugeteilt, um seiner Aufgabe nachkommen zu können.
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Keine festgelegten Fristen, meist Systemparameter, ausschließlich die Geschäftsführung
1.4	Pseudonymisierung	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt gemacht. Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogene Webschulungen. Auf die Besonderheiten im Umgang mit pseudonymisierten Daten wurde hingewiesen.
	Welche technischen Maßnahmen oder Hilfsmittel sind bei der Pseudonymisierung von personenbezogenen Daten im Einsatz?	Die Kundendaten werden bei der Übertragung zwischen der Softwareanwendung des Kunden und unserem Rechenzentrum von DigitalOcean mit TLS v1.2 verschlüsselt.
2	**Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**	
2.1	**Weitergabekontrolle**	
	Wie wird die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten gewährleistet?	Es werden möglichst keine personenbezogenen Daten der Kunden weitergegeben. Einzig im Zuge einer Auftragsverarbeitung, die jedoch vertraglich durch den Art. 28 DSGVO abgesichert wird.
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	Im Rechenzentrum von DigitalOcean werden Informationen mit dem Advanced Encryption Standard (AES) verschlüsselt. Die von DigitalOcean gespeicherten Kundendaten werden während der Übertragung zwischen der Softwareanwendung des Kunden und DigitalOcean mit TLS v1.2 verschlüsselt.
	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	Mit den Auftragsverarbeitern werden AV-Verträge geschlossen.
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.
2.2	**Eingabekontrolle**	
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Rollen-/Rechtekonzepte und diverse Lizenz-modelle mit unterschiedlichen Berechtigungs-konzepten
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß den Weisungen des Auftraggebers erfolgen kann?	Zugriffskontrolle anhand des Rollen-/Rechte-konzepts zur ordnungsgemäßen Datenverarbeitung und Speicherung.
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang die Verarbeitung personenbezogener Daten des Auftraggebers durchführen?	Sämtliche Unterauftragnehmer unterliegen den gleichen Vorgaben wie der Auftragnehmer. Entsprechende Verträge sind geschlossen. Die Pflichten zur Überprüfung der Unterauftrag-nehmer übernimmt der Datenschutzbeauftragte des Unternehmens. Er ist auch bei der Auswahl der beauftragten Firmen maßgeblich beteiligt.
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Festlegung durch Vertragsbindung, bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert.
3	**Verfügbarkeit und Belastbarkeit**	
3.1	**Verfügbarkeitskontrolle**	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Gesicherte Daten sind räumlich von Produktivdaten getrennt.
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Ständig aktuelle Virenscanner und Spamfilter finden Einsatz. Die Systeme werden regelmäßig upgedatet.

	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor der Entsorgung
3.2	**Wiederherstellbarkeit**	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO)	Regelmäßige Backups, USV als auch ein Wiederanlaufkonzept im Rechenzentrum.
4.	**Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)**	
	Welche Verfahren gibt es zur regelmäßigen Bewertung/ Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Der externe Datenschutzbeauftragte überprüft jährlich die Einhaltung der technisch-organisatorischen Maßnahmen. Das Rechenzentrum DigitalOcean hat ein Sicherheitskontrollsystem entwickelt und implementiert, um die Vertraulichkeit, Integrität und Verfügbarkeit der Kundensysteme zu schützen. Die Kundendaten-Nutzungsrichtlinie von DigitalOcean regelt die Anforderungen für die Nutzung von Kundendaten in Übereinstimmung mit verschiedenen Branchenstandards. Das Rechenzentrum ist nach ISO27001 zertifiziert.
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Per Kontaktformular oder per Mail können Anfragen und Probleme dem Team direkt gemeldet werden.
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Keine Vorbelegung durch Haken; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen
4.1	**Auftragskontrolle**	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsverarbeitung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den aktuellen gesetzlichen Vorgaben zur Auftragsverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollpflichten wahr.

Anlage 3 – Anhang 2
Genehmigte Unterauftragnehmer

Der Auftraggeber genehmigt den Einsatz der nachfolgend aufgeführten Unterauftragnehmer des Auftragnehmers:

Name des Unterauftragnehmers	Anschrift/Land	Leistungsinhalt	Angaben zu geeigneten Garantien für Datenübermittlung ins Drittland