Vertragsbedingungen der Zeppelin Rental GmbH („ZRD"),
Graf-Zeppelin-Platz 1, 85748 Garching b. München
zur Verarbeitung von personenbezogenen Daten im Auftrag

1. Geltungsbereich, Datenschutzbedingungen des Geschäftspartners, Änderungen

1.1 Diese Vertragsbedingungen zur Auftragsverarbeitung (nachfolgend „Vereinbarung" genannt) gelten für sämtliche Angebote und Leistungen der ZRD (nachfolgend „Auftragnehmer" genannt) im Zusammenhang mit dem online Kundenportal (https://rentalcenter.zeppelin-rental.de/) der ZRD (nachfolgend „Rental Center" genannt), deren Bestandteil die Verarbeitung von personenbezogenen Daten des Geschäftspartners (nachfolgend „Auftraggeber" genannt) durch den Auftragnehmer ist und der Auftraggeber Unternehmer (§ 14 BGB), eine juristische Person des öffentlichen Rechts oder ein öffentliches Sondervermögen ist.

1.2 Mit Abschluss des ersten Vertrages, in den diese Vereinbarung einbezogen wird, oder mit Zustimmung zu diesen Vertragsbedingungen im Rental Center erkennt der Auftraggeber deren Geltung zugleich für alle künftigen Verträge an, die er mit dem Auftragnehmer (auch mündlich oder per E-Mail) hinsichtlich der im Rental Center vorhandenen Services abschließt, sofern die Services auch die Verarbeitung von personenbezogenen Daten im Auftrag beinhalten. Die jeweils aktuelle Fassung dieser Vereinbarung steht im Rental Center (https://rentalcenter.zeppelin-rental.de/dataprotection) zum Download bereit und wird dem Kunden auf Verlangen übermittelt.

1.3 Für die Verarbeitung von personenbezogenen Daten durch den Auftragnehmer im Auftrag des Auftraggebers gilt ausschließlich diese Vereinbarung. Abweichende, entgegenstehende oder zusätzliche vertragliche Bedingungen des Auftraggebers werden nicht Vertragsinhalt. Dies gilt auch dann, wenn der Auftragnehmer die Leistung an den Auftraggeber in Kenntnis etwaiger Bedingungen des Auftraggebers dieser Vereinbarung des Auftraggebers vorbehaltlos ausführt.

1.4 Von dieser Vereinbarung abweichende Vereinbarungen bedürfen zu ihrer Wirksamkeit der ausdrücklichen Bestätigung in Textform im Sinne von § 126 b BGB (z. B. Brief, E-Mail, Telefax).

2. Gegenstand des Auftrags, Art, Zweck und Umfang der Datenverarbeitung

2.1 Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten (gem. Art. 28 Abs. 3 DS-GVO) durch den Auftragnehmer im Auftrag und nach Weisung des Auftraggebers. Sämtliche Vorgaben dieser Vereinbarung sind einzuhalten.

2.2 Die vom Auftragnehmer zur Erfüllung der vertraglichen Verpflichtungen zu verwendeten Daten und der Kreis der Betroffenen sind:

(a) Vorname, Nachname, Kontaktdaten, Kundenhistorie, mietbezogene Daten (bspw. Mietbeginn und -ende, Vertragsnummern, Ort) und Telemetrie-Daten (bspw. GPS-Standort, Betriebsstunden, Kraftstoffverbrauch)
(b) Firmenkunden, ehemalige Kunden, Mitarbeiter (einschließlich Auszubildende. Praktikanten, Werkstudenten), Lieferanten, Ansprechpartner (z. B. bei Kunden) oder Lieferanten), Nachunternehmen

Der Auftragnehmer verarbeitet die vorgenannten Daten zu erbringen der nachfolgend aufgezählten Services, sofern diese durch den Auftraggeber beauftragt wurden und genutzt werden:

(a) Kontaktdaten: Die Kontaktdaten des Kunden werden verarbeitet, um ihm die Möglichkeit zu geben, sich auf unserer Plattform einzuloggen und unsere Dienste und Services in Anspruch zu nehmen.
(b) Mietbezogene Daten: Mietbezogene Daten des Kunden werden verarbeitet, um einen verbesserten Service bereitzustellen
(c) Telemetrie-Daten: Telemetrie-Daten werden verarbeitet, um dem Kunden einen besseren Überblick über den Zustand und die Leistung seiner Maschinen zu ermöglichen und um einen verbesserten Service bereitzustellen.

2.3 Die Tätigkeit des Auftragnehmers im Rahmen dieser Vereinbarung bestimmt sich aus der konkreten Tätigkeitsbeschreibung in Ziff. 2.2, ergänzender Einzelweisungen sowie dem zwischen den Parteien bestehenden Angeboten, Nutzungsbedingungen und/oder Verträgen (nachfolgend zusammen „Vertrag" genannt), in dessen Ergänzung diese Vereinbarung zur Auftragsverarbeitung geschlossen wird.

3. Verantwortlichkeit Auftraggeber und Weisungsgebundenheit Auftragnehmer

3.1 Allein der Auftraggeber ist für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchgeführten Verarbeitung personenbezogener Daten durch den Auftragnehmer im Hinblick auf die jeweils anwendbaren Bestimmungen des Datenschutzrechts verantwortlich.

3.2 Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers nur auf Weisung des Auftraggebers. Der Auftragnehmer ist nicht berechtigt, die Daten des Auftraggebers in einer Weise zu verarbeiten, die diesen Vorgaben widersprechen. Ausgenommen hiervon ist die Verarbeitung von anonymisierten Daten zu statistischen Zwecken sowie zur Verbesserung der Services des Auftragnehmers.

3.3 Der Auftraggeber weist den Auftragnehmer an, die personenbezogenen Daten zum Zweck der Erbringung der vereinbarten Leistungen/ Services zu verarbeiten, wie in etwaigen Vereinbarungen, Angeboten, Nutzungsbedingungen sowie in dieser Vereinbarung beschrieben. Diese Vereinbarung inkl. ihrer Anlage stellt gemeinsam mit den zu den Leistungen /Services getroffenen Vereinbarungen / Verträge die abschließenden Weisungen an den Auftragnehmer zum Zeitpunkt des Vertragsschlusses dar.

3.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.5 Ziff. 3.2 wird eingeschränkt, soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu einer Datenverarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (vgl. Art. 28 Abs. 3 a) DSGVO).

4. Weisungen und weisungsberechtigte Personen

4.1 Der Auftraggeber oder ein entsprechend Bevollmächtigter werden sämtliche Weisungen in Textform (schriftlich oder E-Mail) erteilen. Sofern ausnahmsweise mündliche Weisungen erteilt werden, müssen diese umgehend schriftlich oder per E-Mail bestätigt werden.

4.2 Soweit Weisungen oder Hinweise nach dieser Vereinbarung gegenüber der anderen Partei zu erfolgen haben, sind diese an die im Vertrag genannten Personen zu richten. Jede Partei kann die angegebenen Kontaktpersonen durch Erklärung in Textform gegenüber der anderen Partei ändern. Die Änderung wird umgehend nach Zugang der Änderungserklärung wirksam.

5. Pflichten des Auftragnehmers

5.1 Eine Berichtigung, eine Löschung von Daten oder eine Einschränkung der Verarbeitung ist dem Auftragnehmer nicht gestattet, es sei denn, es liegt eine entsprechende Weisung vor. Anträge von Betroffenen auf Berichtigung, Löschung oder Sperrung sind an den Auftraggeber weiterzuleiten.

5.2 Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Falls eine Ausnahme vom Auftraggeber genehmigt wurde, muss ein angemessenes Schutzniveau sichergestellt werden, das die Vorgaben der Art. 44 ff. DSGVO erfüllt. Erfolgt die Verarbeitung in einem Drittland durch Sub-Dienstleister, erklärt sich der Auftraggeber damit einverstanden, dass der Auftragnehmer die Erfüllung der Vorgaben der Art. 44 ff. DSGVO sicherstellen kann, indem er z.B, die Standardvertragsklauseln verwendet, die von der Kommission gemäß Artikel 46 Abs. 2 c) DSGVO erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

5.3 Der Auftragnehmer führt ein Verzeichnis von Verarbeitungstätigkeiten für alle im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeiten, das die Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Soweit der Auftraggeber Informationen von dem Auftragnehmer benötigt, um sein Verzeichnis von Verarbeitungstätigkeiten vollständig erstellen zu können, wird der Auftragnehmer die Informationen auf Anforderung bereitstellen. Gleiches gilt bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers. Der Auftragnehmer ist verpflichtet, im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich zu unterstützen.

5.4 Der Auftragnehmer wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

5.5 Der Auftragnehmer ist verpflichtet sicherzustellen, dass seine Mitarbeiter, die Zugang zu personenbezogenen Daten im Rahmen der Auftragserfüllung haben, diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten. Dies gilt nicht, wenn der Dienstleister nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung der vertragsgegenständlichen personenbezogenen Daten verpflichtet ist.

5.6 Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen vorab zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

5.7 Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) erforderlichen Maßnahmen unterstützen.

5.8 Der Auftragnehmer hat – sofern er hierzu gesetzlich verpflichtet ist – einen qualifizierten Beauftragten für den Datenschutz bestellt. Auf Anfrage stellt der Auftragnehmer dem Auftraggeber die Kontaktdaten zur Verfügung. Der Auftragnehmer kann sich auch direkt per E-Mail an dataprivacy@zeppelin.com wenden.

5.9 Der Auftragnehmer soll den Auftraggeber per E-Mail unverzüglich ab Kenntnisnahme von jedwedem Empfang von Anfragen oder Aufforderungen, die von einer Datenschutzaufsichtsbehörde bezüglich des Gegenstandes dieser Vereinbarung gemacht wird, informieren.

5.10 Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO verantwortlich. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten, insbesondere auf Auskunft, Berichtigung, Einschränkung, Datenübertragbarkeit oder Löschung erforderlich ist, wird der Auftragnehmer die gem. Art. 28 Abs. 3 lit. e DSGVO jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber über entsprechende Anfragen von Betroffenen unverzüglich informieren.

6. Sub-Dienstleister

6.1 Die Einbeziehung von Sub-Dienstleistern in die vertragsgegenständliche Datenverarbeitung ist nur mit Zustimmung des Auftraggebers zulässig. Der Auftragnehmer wird dem Auftraggeber die Einbeziehung von Sub-Dienstleistern vorab in Textform ankündigen. Widerspricht der Auftraggeber diesem Einsatz nicht innerhalb von 4 Wochen nach der Anzeige, gilt die Zustimmung des Auftraggebers als erteilt. Für die folgend angeführten Sub-Dienstleister gilt die Zustimmung auch unter Berücksichtigung von Ziff. 4.2 als erteilt:

- Computer Manufaktur GmbH, Franklinstraße 11, 10587 Berlin, Tätigkeitsbereich: Entwicklung und Wartung des Frontend-Bereichs
- Zeppelin GmbH, Graf-Zeppelin-Platz 1, 88045 Friedrichshafen, Tätigkeitsbereich: Entwicklung und Wartung einer Schnittstelle zur Verarbeitung von Telemetrie-Daten

6.2 Über beabsichtigte Änderungen in Bezug auf die Ersetzung oder Hinzuziehung weiterer Sub-Dienstleister wird der Auftragnehmer den Auftraggeber informieren. Der Auftraggeber kann im Einzelfall Einspruch gegen die Beauftragung eines Sub-Dienstleisters aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erheben. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt das Einspruchsrecht in Bezug auf den konkreten Sub-Dienstleister. Erhebt der Auftraggeber berechtigten Einspruch gegen die Hinzuziehung eines Sub-Dienstleisters, ist der Auftragnehmer befugt, der zugrundeliegende Vertrag und diese Vereinbarung mit einer Frist von einem Monat zum Monatsende zu kündigen.

6.3 Sofern eine Beauftragung erfolgt, hat der Auftragnehmer den Sub-Dienstleister im Hinblick auf die Erfüllung der vertraglichen Verpflichtungen sorgfältig auszuwählen. Er hat die vertraglichen Vereinbarungen mit dem Sub-Dienstleister so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer entsprechen. Insbesondere hat er gegenüber seinen Sub-Dienstleistern die in dieser Vereinbarung geregelten Verfügungsberechtigungen und die Kontrollrechte des Auftraggebers vertraglich abzusichern.

6.4 Der Auftragnehmer hat sicherzustellen, dass auch bei den Tätigkeiten des Sub-Dienstleisters die Datenschutzvorschriften über die Auftragsverarbeitung sowie die sich für den Auftragnehmer aus dieser Vereinbarung ergebenden Pflichten auch im Unterauftragsverhältnis beachtet werden.

6.5 Nicht als genehmigungspflichtige Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigung, Prüfungen oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

7. Festlegung der technischen und organisatorischen Maßnahmen

7.1 Die Auswahl des Auftragnehmers erfolgt insbesondere aufgrund der Einschätzung, dass er hinreichende Garantien dafür bietet, die technischen und organisatorischen Maßnahmen zur Datensicherheit einzuhalten und die Verarbeitung der personenbezogenen Daten im Einklang mit Anforderungen der gesetzlichen Regelungen vorzunehmen und den Schutz der Rechte der Betroffenen zu gewährleisten.

7.2 Der Auftragnehmer stellt die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der zur Datenverarbeitung eingesetzten Systeme und Dienste sicher. Der Auftragnehmer gewährleistet für seinen Verantwortungsbereich die Umsetzung der angemessenen technischen und organisatorischen Maßnahmen entsprechend den in **Anlage TOMs** getroffenen Regelungen, um die Einhaltung der Datenschutzvorschriften zu gewährleisten.

7.3 Der Auftragnehmer gewährleistet für seinen Verantwortungsbereich gemäß dem jeweiligen Stand der Technik die Umsetzung der angemes-

senen technischen und organisatorischen Maßnahmen zur Einhaltung der Datenschutzvorschriften und dauerhaften Eindämmung des Risikos, das mit der Datenverarbeitung verbunden ist. Das in der **Anlage TOMs** beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach dem Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar und wird verbindlich festgelegt.

7.4 Die Verarbeitung von Daten in Privatwohnungen ist grundsätzlich gestattet. Zulässig ist insbesondere die temporäre Zwischenspeicherung durch den Einsatz von mobilen Geräten (z. B. Laptops, Tablet-PCs, Smartphones etc.), sofern die mobilen Geräte über ausreichende, den anerkannten Standards entsprechende Sicherungseinrichtungen (z. B. VPN-Anbindung, Festplattenverschlüsselung etc.) verfügen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesen Fällen sicherzustellen.

7.5 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

8. Mitzuteilende Verstöße des Auftragnehmers / Datenverlust

8.1 Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass eine Verletzung des Schutzes der von ihm für den Auftraggeber verarbeiteten Daten personenbezogenen Daten gem. Art. 4 Nr. 12 DSGVO vorliegt („Datensicherheitsvorfall"), hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten.

8.2 In Hinblick auf eventuelle Informationspflichten des Auftraggebers gegenüber Aufsichtsbehörden für den Datenschutz und/oder den Betroffenen hat der Auftragnehmer den Auftraggeber unverzüglich über sämtliche Vorfälle zu informieren, bei denen nicht auszuschließen ist, dass Daten abhandengekommen oder anderweitig Dritten unberechtigt zur Kenntnis gelangt sind. In diesem Fall kann der Auftraggeber die Mitwirkung des Auftragnehmers an der Aufarbeitung des Zwischenfalls verlangen.

9. Kontrolle durch den Auftraggeber

9.1 Der Auftraggeber oder ein entsprechend Beauftragter haben das Recht, die Befolgung sämtlicher Weisungen und Bestimmungen dieser Vereinbarung sowie der datenschutzrechtlichen Vorgaben, soweit sie auf die vertragsgegenständliche Datenverarbeitung anwendbar sind, durch den Auftragnehmer zu den üblichen Geschäftszeiten (montags bis freitags 10 bis 18 Uhr) auf eigene Kosten zu kontrollieren. Vor Ort durchgeführte Inspektionen sind gegenüber dem Auftragnehmer angemessene Zeit vorher (in der Regel mindestens 14 Tag) anzukündigen. Der Auftragnehmer hat das Recht, Kontrollpersonen aus begründetem Anlass (z. B. bei Bestehen eines Wettbewerbsverhältnisses) abzulehnen. Der Auftragnehmer verpflichtet sich, entsprechende Überprüfungen zu dulden und dem Auftraggeber bei Kontrollen zu unterstützen sowie die erforderlichen Auskünfte zu erteilen. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere ohne begründeten Anlass angeordnete Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

9.2 Der Auftraggeber nimmt angemessen Rücksicht auf die Betriebsabläufe und Interessen des Auftragnehmers unter strikter Geheimhaltung der Geschäftsgeheimnisse. Externe Prüfer verpflichtet der Auftraggeber zur Verschwiegenheit und Geheimhaltung, soweit diese nicht einer beruflichen Verschwiegenheitsverpflichtung unterliegen.

9.3 Nach Wahl des Auftragnehmers, kann der Nachweis der Einhaltung der Pflichten nach dieser Vereinbarung anstatt durch eine Inspektion auch durch Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT Sicherheitsabteilung oder Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT- Sicherheits- oder Datenschutzaudit – z. B. nach BSI-Grundschutz – („Prüfbericht") erbracht werden, wenn der Prüfbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

9.4 Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Verpflichtungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, über Kosten, zu Qualitäts-, Vertrags- und Managementberichten sowie zu anderen vertraulichen Daten des Auftragnehmers zu erhalten, soweit diese nicht unmittelbar relevant für die vereinbarten Datenverarbeitungen sind.

9.5 Gemäß den anwendbaren Datenschutzvorschriften unterliegen der Auftraggeber und der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Verlangen des Auftraggebers wird der Auftragnehmer im Rahmen von örtlichen Aufsichtsverfahren nach Kräften unterstützen, wenn und soweit die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten Gegenstand des Aufsichtsverfahrens ist.

10. Laufzeit und Kündigungsrecht

10.1 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der beauftragten Leistungen / Services. Die Regelungen zur ordentlichen Kündigung in den Vereinbarungen zu den Leistungen / Services gelten entsprechend.

10.2 Das Recht der der Parteien zur außerordentlichen Kündigung der Vereinbarung bei schwerwiegenden Vertragsverstößen bleibt davon unberührt.

11. Löschung

11.1 Nach Erbringung der vereinbarten Leistungen/Services oder nach Aufforderung durch den Auftraggeber, spätestens jedoch mit Kündigung und Beendigung der Leistungen/Services, hat der Auftragnehmer sämtliche noch in seinem Besitz befindlichen personenbezogenen Datenbestände, die im Zusammenhang mit dem Vertragsverhältnis mit dem Auftraggeber stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, soweit die Daten nicht dem Nachweis der auftrags- und ordnungsgemäßen Leistungserbringung oder gesetzlichen Aufbewahrungspflichten unterliegen.

11.2 Im Falle der Löschung der personenbezogenen Daten bestätigt der Auftragnehmer dem Auftraggeber die vollständige und unwiderruflich Löschung der Daten auf Anforderung. Die Löschung/Vernichtung ist in geeigneter Weise – etwa durch eine Protokollierung – zu dokumentieren.

12. Nebenabreden und anwendbares Recht

12.1 Mündliche Nebenabreden sind nicht getroffen. Sämtliche Änderungen oder Ergänzungen dieser Datenschutzvereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für dieses Schriftformerfordernis.

12.2 Diese Datenschutzvereinbarung unterliegt deutschem Recht unter Ausschluss des UN-Kaufrechts.

12.3 Erfüllungsort und Gerichtsstand für sämtliche sich zwischen den Vertragsparteien aus dieser Vereinbarung ergebenden Verpflichtungen bzw. Streitigkeiten ist, soweit der Auftraggeber Vollkaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist, sowie für den Fall, dass der Auftraggeber keinen Gerichtsstand im Inland hat, München.

13. Anlagen

Anlage TOMs Vorgaben zur Datensicherheit ist Bestandteil des Vertrages.

Stand Oktober 2023

Anlage TOMs: Vorgaben zur Datensicherheit

Für die konkrete Datenverarbeitung wird ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Die nachfolgend beschriebenen Maßnahmen stellen die Auswahl der technischen und organisatorischen Maßnahmen („**TOM**") zur Gewährleistung der Datensicherheit nach Art. 32 DSGVO passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik dar.

I. Organisatorische Vorgaben zur Gewährleistung der Datensicherheit

Der Auftragnehmer unterhält ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung. Hierdurch soll auch sichergestellt werden, dass die getroffenen Maßnahmen zur Gewährleistung der Datensicherheit dem Stand der Technik entsprechen. Die organisatorischen Vorgaben als auch deren Umsetzung werden auf Anfrage jederzeit dem Auftraggeber nachgewiesen.

II. Technische Maßnahmen zur Gewährleistung der Datensicherheit

Der Auftragnehmer trifft zur Gewährleistung der Datensicherheit folgende Maßnahmen, deren Einhaltung durch entsprechende Kontrollen im Rahmen der organisatorischen Maßnahmen gewährleistet wird:

1. Vertraulichkeit

Es ist sicherzustellen, dass keine Person – sowohl Mitarbeiter als auch Dritte – personenbezogene Daten unbefugt zur Kenntnis nimmt. Die Sicherstellung dieses Schutzziels erfordert Maßnahmen zur Zutritts-, Zugangs- und Zugriffskontrolle. Ein unbefugter Gerätezugriff soll unterbunden werden. Zudem werden hier auch die Vorgaben zur Mandantentrennung angeführt, um sicherzustellen, dass eine Zuordnung von Daten zu einem Verantwortlichen erfolgt.

a) Zutrittskontrolle:

Kontrolle des räumlichen Zutritts zu Datenverarbeitungsanlagen (DV-Anlage) durch Unbefugte. Durch die Zutrittskontrolle soll verhindert werden, dass Personen, die dazu nicht befugt sind, in die Nähe einer DV-Anlage gelangen können. Zur DV-Anlage gehören neben den Servern auch die angeschlossenen Speichermedien und Endgeräte. Auch die für einen Fernzugriff genutzten Endgeräte werden erfasst.

Hierfür verpflichtet sich der Auftragnehmer mindestens die folgenden Maßnahmen zu ergreifen:

- Gebäudesicherheitskonzept
- Zutrittsberechtigungskonzept
- Einsatz eines Zutrittskontrollsystems
- Sperrung des Zutritts nach Ablauf der Berechtigung

b) Zugangskontrolle:

Die Benutzung von DV-Anlagen durch unbefugte Personen (nicht befugte Mitarbeiter oder Externe) soll verhindert werden. Bei der Zugangskontrolle geht es um die Frage der Identifikation und anschließender Authentifikation. Die Zugangskontrolle umfasst auch das Ziel, dass kein externer Zugang (z. B. aus dem Internet) auf DV-Anlagen erfolgen kann (Hackerschutz).

Hierfür verpflichtet sich der Auftragnehmer mindestens die folgenden Maßnahmen zu ergreifen:

- Authentisierung der Benutzer gegenüber dem Datenverarbeitungssystem.
- Verwendung von individuellen Benutzerkennungen und Passwörtern
- Passwortpolicy mit Mindestvorgaben zur Passwortkomplexität, -länge und Änderungsintervalen
- Verpflichtung zur Vertraulichkeit
- Protokollierung und Auswertung der Systembenutzung
- Abschottung interner Netze gegen Zugriffe von außen (Firewalls, VPN, starke Authentifizierung aus dem Internet)
- Absicherung von Netzwerkzugängen (WLAN, LAN)

c) Zugriffskontrolle:

Ziel der Zugriffskontrolle ist es, dass Mitarbeiter und befugte Dritte nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können. Darüber hinaus soll sichergestellt werden, dass beim Umgang mit personenbezogenen Daten diese nicht unbefugt gelesen, kopiert, verändert oder entfernt (gelöscht) werden können. Dies gilt sowohl für Daten, die in DV-Systemen gespeichert sind, als auch für solche, die sich auf maschinell lesbaren Datenträgern oder auf Papier befinden.

Hierfür verpflichtet sich der Auftragnehmer mindestens die folgenden Maßnahmen zu ergreifen:

- Festlegung der Zugriffsberechtigung, Berechtigungskonzept
- Dokumentierte Vergabe von Berechtigungen an Mitarbeiter und Erfüllungsgehilfen nach dem Minimalprinzip; Zugriff auf Anwendungen und Systemkomponenten wird nur gestattet, wenn dieser Zugriff für die konkrete Tätigkeit erforderlich ist.
- Reduzierung privilegierter Nutzer auf ein Minimum (Administratoren)
- Einsatz von Sicherheitssystemen (z. B. Virenscanner, Firewalls, SPAM-Filter)
- Umsetzung eines Schwachstellen- und Patchmanagements
- Regelungen zum Umgang mit Informationen (Datenklassifizierung, Clean Desk Policy)
- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger nach dem jeweiligen Stand der Technik unter Beachtung der jeweils gültigen Normen (DIN 66399:2012) oder Beauftragung eines auf Entsorgung von Datenträgern spezialisierten Dienstleisters mit der Entsorgung, der die Datenträger mit derselben oder einer höheren Sicherheitsstufe vernichten wird.

d) Trennungskontrolle:

Nach dem Trennungsgebot sind Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt zu verarbeiten (auch: Gebot der Nichtverkettbarkeit). Dadurch soll gewährleistet werden, dass die Zweckbindung personenbezogener Daten durch organisatorische und technische Maßnahmen umgesetzt wird. Besondere Bedeutung hat das Trennungsgebot im Rahmen der Auftragsverarbeitung, wenn z. B. Daten mehrerer Auftraggeber auf einem System gespeichert sind. Sofern das Trennungsgebot nicht durch technische Maßnahmen, wie z. B. eine Zugriffs-Kontroll-Software, erreicht werden kann, ist eine getrennte Speicherung notwendig.

Hierfür verpflichtet sich der Auftragnehmer mindestens die folgenden Maßnahmen zu ergreifen:

- Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt
- Funktionstrennung
- Trennung von Entwicklungs-, Test und Produktivsystem

2. Integrität

Es ist sicherzustellen, dass informationstechnische Prozesse und Systeme die festgelegten Spezifikationen kontinuierlich einhalten, so dass die mit ihnen zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben.

a) Weitergabekontrolle:

Umfasst sind alle Varianten der Weitergabe von personenbezogenen Daten mittels Datenträger oder Kommunikationsnetz. Die Weitergabekontrolle soll verhindern, dass Daten bei deren Weitergabe unbefugt verwendet (gelesen, kopiert, verändert oder entfernt/gelöscht) werden können. Der Begriff der Weitergabe umfasst sowohl die Übermittlung an Dritte als auch die Weitergabe im Rahmen der Auftragsverarbeitung zwischen Auftraggeber und Auftragnehmer und an den Betroffenen.

Hierfür verpflichtet sich der Auftragnehmer mindestens die folgenden Maßnahmen zu ergreifen:

- Authentisierte und hinreichend verschlüsselte Übertragung von Daten vor der Weitergabe bei nicht gesicherten Übertragungswegen

b) Eingabekontrolle:

Durch die Eingabekontrolle soll dokumentiert werden, wer für eine (un) zulässige oder fehlerhafte Dateneingabe verantwortlich ist. Ziel ist die Revisionsfähigkeit der Eingabe von personenbezogenen Daten in das DV-System, zu welchem auch nicht vernetzte Einzelarbeitsplätze, wie z. B. PCs gehören. Die zu kontrollierende Dateneingabe umfasst sowohl das erstmalige Speichern als auch die Veränderung und Löschung (Entfernung) von Daten.

Hierfür verpflichtet sich der Auftragnehmer mindestens die folgenden Maßnahmen zu ergreifen:

- Festlegung von Benutzerprofilen
- Differenzierte Benutzerberechtigungen: Lesen/Ändern/Löschen
- Verpflichtung auf das Datengeheimnis
- Löschungsregelung für Protokolldaten

3. Verfügbarkeit und Belastbarkeit

Die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall muss rasch wiederherzustellen sein. Dazu ist der Schutz der Daten gegen zufällige Zerstörung oder Verlust zu gewährleisten. Mögliche Gefahren sind z. B. Wasserschäden, Blitzschlag, Stromausfall, Brand, Sabotage oder Diebstahl. Mit dem Schutzziel der Belastbarkeit soll eine gewisse Stabilität gegenüber Ausfällen und Angriffen der Systeme erreicht werden. Da diese Anforderung auch besondere Relevanz bei der Auslagerung von Dienstleistungen (Hosting von Daten) hat, werden auch hier die Anforderungen an eine Auftragskontrolle mit angeführt.

a) Auftragskontrolle:

Gewährleistung der weisungsgemäßen Auftragsverarbeitung. Der Auftragnehmer hat die ihm erteilten Weisungen einzuhalten, während der Auftraggeber Sorge dafür zu tragen hat, dass seine Weisungen klar und eindeutig sind und befolgt werden.

Hierfür verpflichtet sich der Auftragnehmer mindestens die folgenden Maßnahmen zu ergreifen:

- Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)
- Zentrale Erfassung vorhandener Auftragsverarbeiter (einheitliches Vertragsmanagement)
- Kontrolle der Einhaltung von Datensicherheitsbestimmungen durch Auftragnehmer und Meldung, wenn Verstöße vorliegen oder der Verdacht besteht, dass die Datensicherheitsvorgaben unzureichend sind.
- Sichtung vorhandener IT-Sicherheitszertifikate der Subunternehmer

b) Verfahren zur regelmäßigen Überprüfung

Ständige Gewährleistung der Einhaltung der Vorgaben an Datenschutz und IT-Sicherheit. Der Auftragnehmer hat regelmäßig zu überprüfen und dokumentieren, dass die vertraglich geschuldeten Vorgaben eingehalten werden.

Hierfür verpflichtet sich der Auftragnehmer mindestens die folgenden Maßnahmen zu ergreifen:

- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten
- Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert
- Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen Kontrolle unterzogen
- Es werden datenschutzfreundliche Voreinstellungen gewählt
- Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt
- Regelmäßige Kontrolle der Wirksamkeit der durchgeführten Maßnahmen

Stand Oktober 2023