Auftragsverarbeitung

gemäß Art. 28 DSGVO im Rahmen der Nutzung von CI-Cloud-Portal und den damit verbundenen Diensten.

zwischen

Bitte geben Sie Firmenname mit dazugehöriger Anschrift hier an.

- Auftraggeber -

und

ci solution GmbH
Andreas Stäblein Straße 14
97280 Remlingen

E-Mail: info@ci-solution.com
Tel.: +49 9369 / 980441
Fax: +49 9369 / 980443

- Auftragnehmer -

Präambel

Zwischen den Parteien besteht ein Vertragsverhältnis im Rahmen der Nutzung von CI-Cloud-Portal und den damit verbundenen Diensten der ci solution GmbH:

- CI-Out-of-Office Lite
- CI-Sign
- CI-ExtendRuleset
- CI-Archive
- CI-Signature Add-In
- CI-Disclaimer
- CI-Out-of-Office Manager

Diese Vereinbarung dient als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere des Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO).

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus der Nutzung von CI-Cloud Portal (im Folgenden Leistungsvereinbarung)

(2) Die Dauer des Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

(3) Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

3. Konkretisierung des Auftragsinhalts

(1) Über das CI-Cloud Portal werden E-Mail Signaturen und Disclaimer an ausgehende E-Mails des Auftraggebers angefügt.

Hierbei werden E-Mails über einen sogenannten Connector von dem Office 365 Tenant des Auftraggebers an die Server des Auftragnehmers übermittelt. Hier werden die E-Mails um eine Signatur / Disclaimer ergänzt und anschließend wieder zurück an den Office 365 Tenant geleitet. Alternativ kann auch ein abweichender Relay Server angegeben werden, z.B. eine Appliance Lösung. Die Verarbeitung der E-Mails durch den Auftragnehmer erfolgt ausschließlich innerhalb der ISO 27001-zertifizierten Microsoft Azure Infrastruktur (https://www.microsoft.com/de-de/TrustCenter/Compliance/ISO-IEC-27001). Somit ist gewährleistet, dass E-Mails im Zuge der Verarbeitung durch den Auftragnehmer die Microsoft Azure Infrastruktur nicht verlassen.

Die Verarbeitung von E-Mails durch den Auftragnehmer erfolgt ausschließlich für vom Auftraggeber versendete E-Mails. Empfangene (eingehende) E-Mails werden nicht an den Auftragnehmer weitergeleitet und nicht verarbeitet.

Darüber hinaus, kann der Personenkreis dessen E-Mails durch den Auftragnehmer verarbeitet werden über eine Active Directory Sicherheitsgruppe eingeschränkt werden. Diese Einschränkung greift auf Connector-Ebene innerhalb des Office 365 Tennant des Auftraggebers, so dass E-Mails gar nicht erst an die Server des Auftragnehmers weitergeleitet werden.

(2) Bei Verwendung des Cloud-Standort „Northeurope“ (konfigurierbar über „Unternehmensprofil“ innerhalb von CI-Cloud-Portal) findet die Erbringung der vertraglich vereinbarten Datenverarbeitung ausschließlich 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 Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(3) Technischer Support / Betreuung
Während der gesamten Laufzeit des Hauptvertrages unterstützt und begleitet der Auftragnehmer den Auftraggeber im Rahmen des technischen Support sowie der Kundenbetreuung. Art und Umfang dieser Leistungen können in Umfang und Ausführung variieren.

- Der Auftragnehmer unterstützt den Auftraggeber bei Fragen und Problem im Umgang mit der Software. Die Unterstützung erfolgt in der Regel per E-Mail, Telefon oder über Fernwartung.

- Der Auftragnehmer unterstützt den Auftraggeber bei der Einrichtung und Konfiguration der Software. Die Unterstützung erfolgt in der Regel per E-Mail, Telefon oder über Fernwartung.
- Der Auftragnehmer beantwortet Fragen zur Software per E-Mail oder per Telefon.
- Der Auftragnehmer untersucht Protokoll und Log-Dateien um Fehler in der Software bzw. beim Betrieb der Software zu lokalisieren und zu beheben. Die Unterstützung erfolgt in der Regel per E-Mail, Telefon oder über Fernwartung.
- In besonderen Fällen (z.B. Vor-Ort-Service) findet der Support direkt beim Auftraggeber vor Ort statt.

Für die Fernwartung setzt der Auftragnehmer vorzugsweise Teamviewer ein. Hierbei verfolgt der Auftraggeber die Remote Sitzung live am Monitor. Der Auftragnehmer führt Fernwartungssitzungen nur im Beisein des Auftraggebers durch.

(4) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)

(5) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen

- Kunden
- Interessenten
- Beschäftige
- Lieferanten
- Ansprechpartner

4. Rechte und Pflichten des Auftraggebers

(1) Die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers erfolgt ausschließlich im Rahmen dieser Vereinbarung nebst Anlagen und nach Weisung des Auftraggebers hinsichtlich Art, Umfang und Verfahren der Datenverarbeitung. Änderungen des Verarbeitungsgegenstandes und andere vertraglich festgelegte Rahmenbedingungen sind vertraglich zu vereinbaren und zu dokumentieren. Weisungen können

- schriftlich,
- per Fax
- oder per E-Mail

erfolgen.

(2) Der Auftraggeber kann die von den beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen und die Einhaltung der Anforderungen des Art. 28 DSGVO sowie der übrigen Anforderungen dieser Vereinbarung überprüfen. Der Auftragnehmer unterstützt den Auftraggeber bzw. einen vom Auftraggeber benannten Prüfer hierbei.

Die Kosten für alle Kontrollmaßnahmen hat der Auftraggeber zu tragen. Zu den

Kosten zählen auch die Aufwände, die dem Auftragsverarbeiter auf Grund der durchzuführenden Kontrollen entstehen.

Hiervon ausgenommen sind Aufwände, die

a) aufgrund eines konkreten Gesetzes- oder Vertragsverstoß,

b) aufgrund eines konkreten Datenschutzvorfalles .I.d. Art. 33 DSGVO oder auf Veranlassung einer Aufsichtsbehörde,

c) für eine optionale Nachweiserbringung in Form von Testaten, von Berichten oder Berichtsauszügen unabhängiger Instanzen oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit anfallen.

Die Kosten werden nach tatsächlich angefallenem Aufwand zu 160 € / Stunde, jedoch maximal mit EUR 1280,- netto abgerechnet.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Wartung und Pflege durch den Auftragnehmer feststellt.

5. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, auf die er im Zusammenhang mit den Wartungs-/Pflegearbeiten Zugriff erhält, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(3) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(4) Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

- besondere Arten bzw. besondere Kategorien personenbezogener Daten Art. 9 DSGVO oder
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, 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. Der Auftragnehmer ist darüber hinaus verpflichtet,

unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

6. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber nach Art. 58 DSGVO i.V.m. § 40 BDSG (neu), insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

7. Fernwartung

(1) Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

(2) Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

(3) Bei der Verarbeitung von Daten außerhalb der Geschäftsräume durch in das Projekt einbezogene Mitarbeiter werden die datenschutzrechtlichen Vorschriften eingehalten.

8. Unterauftragsverhältnisse

(1) Die zum Vertragsschluss bestehenden Unterauftragsverhältnisse sind in **Anlage 2 – Unterauftragnehmer** zu diesem Vertrag, mit Namen, Anschrift und Art der Leistung (Kurzbeschreibung), angegeben. Der Auftraggeber erklärt sich damit einverstanden.

(2) Die zukünftige Beauftragung von Unterauftragnehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer ohne gesonderte Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DSGVO. Der Auftragnehmer

informiert den Auftraggeber über jede beabsichtigte Änderung, in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragnehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben, sofern der Auftraggeber hierfür einen sachlichen Grund benennt.

(3) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Eine Beauftragung von Unterauftragnehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 – 49 DSGVO erfüllt sind.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 6 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

9. Datengeheimnis

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter in einer dem Art. 28 Abs. 3 lit. b) genügenden Weise zur Vertraulichkeit verpflichten, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

10. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Melde-pflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

(a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

(b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

(c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

(d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

(e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

(2) Für den Fall, dass der Auftragnehmer die Wartung und Pflege von IT-Systemen für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt, stellt der Auftragnehmer dem Auftraggeber eine Beschreibung der von ihm getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO in geeigneter Weise zur Verfügung. Dies beinhaltet auf Aufforderung des Auftraggebers auch Nachweise über das nach Art. 32 Abs. 1 lit. d) einzurichtende Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

13. Löschung von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien und Cache-Dateien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche Daten und Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen zu löschen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

14. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

15. Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland, wobei die Geltung des UN-Kaufrechts ausgeschlossen wird.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

16. Sonstiges

(1) Gerichtsstand für beide Parteien ist Würzburg.

_____, den _____	_____, den _____
Ort Datum	Ort Datum
_____	_____
– Auftraggeber -	- Auftragnehmer -

Anlage 1 - Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Getroffene Maßnahmen zur Zutrittskontrolle

- Der Firmensitz ist durch verschlossene Türen sowie einer Alarmanlage geschützt. Zugang zu den Geschäftsräumen ist nur Mitarbeitern mit Schlüssel möglich.
- Schlüssel erhalten ausschließlich zutrittsberechtigte Personen. Die Schlüsselvergabe wird protokolliert.
- Die für CI-Cloud Portal eingesetzte IT Infrastruktur wird vollständig auf ISO 27001-zertifizierten Microsoft Azure Servern (https://www.microsoft.com/de-de/TrustCenter/Compliance/ISO-IEC-27001) gehostet und betrieben.
- Der Zugriff auf die in Microsoft Azure betriebene Infrastruktur ist nur über gesicherte Wege (Multi-Faktor-Authentifizierung) und von bestimmten IP Adressen (RDP Zugriff auf Virtual Server) aus möglich.
- Neben den technischen Maßnahmen ist zu erwähnen, dass die ci solution GmbH ein inhabergeführtes und „familiäres“ Unternehmen überschaubarer Größe ist. Die Mitarbeiter kennen sich untereinander – fremde Personen fallen sofort auf.

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Getroffene Maßnahmen zur Zugangskontrolle:

- Alle Systeme sind mindestens durch Passwort, in der Regel aber durch Multi-Faktor-Authentifizierung, geschützt.
- Die Mitarbeiter sind angehalten den Bildschirm beim Verlassen des Arbeitsplatzes zu sperren.
- Eingeräumte Berechtigungen werden periodisch überprüft.
- Berechtigungen werden nur dann eingeräumt, wenn erforderlich.
- IT-Systeme werden durch gängige und aktuelle Software zur Abwehr von Viren und Schadsoftware geschützt.
- Fernzugriff auf IT-Systeme ist grundsätzlich nur über passwortgeschützte VPN, IPSec, SSH, SFTP, SSL/TLS Verbindungen (verschlüsselte, authentifizierte Verbindungen) möglich.

3. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Getroffene Maßnahmen zur Zugriffskontrolle:

- Seitens der ci solution GmbH ist der Zugriff auf die IT-Systeme auf zutrittsberechtigte Personen beschränkt.
- CI-Cloud Portal Dienste werden in Form von Log-Files protokolliert.
- Nicht benötigte Dienste, Ports und Accounts werden standardmäßig deaktiviert/gesperrt.
- Von Kunden im Rahmen des Support zur Verfügung gestellte Log Files und sonstige Daten werden nach Abschluss des Support Case unmittelbar gelöscht.

4. Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welcher Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Getroffene Maßnahmen zur Weitergabekontrolle:

- Die Daten der ci solution Gmbh werden ausschließlich auf gesicherten Systemen gespeichert.
- Die zum Zweck der Fehleranalyse im CI-Cloud Portal automatisch erstellten Log-Files, werden nach 48 Stunden automatisch gelöscht.
- Die Übertragung von Log-Files unserer Desktop Applikationen an uns erfolgt durch den Kunden. Er kann den Übertragungsweg bestimmen. Eine automatische Übertragung erfolgt zu keiner Zeit.
- Nicht mehr benötigte Daten werden nach Abschluss eines Support-Case unmittelbar durch die ci solution GmbH gelöscht.

5. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Getroffene Maßnahmen zur Eingabekontrolle

- Ständige Überwachung durch den Auftraggeber für die Dauer des Remotezugriffs (ggf. auch durch Aufzeichnung seitens Auftraggeber).

6. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Getroffene Maßnahmen zur Auftragskontrolle:

- Verarbeitung gemäß Vertrag des Auftraggebers und den Inhalten dieses Dokumentes.

7. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Getroffene Maßnahme zur Verfügbarkeitskontrolle:

- Datensicherung vor der Verbindung beim Auftraggeber.

8. Zweckbindungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen zur Zweckbindungskontrolle:

- Die ci solution GmbH nimmt ausschließlich die Erfüllung der beauftragten Leistungen durch den Auftraggeber vor.
- Die ci solution GmbH verpflichtet alle Mitarbeiter, die personenbezogene Daten verarbeiten, auf das Datengeheimnis, das Fernmeldegeheimnis nach § 3 TTDSG sowie das Sozialgeheimnis nach § 35 Abs. 1 SGB I.

Aktualisierungen / Verbesserungen

Die genannten Maßnahmen werden regelmäßig unter Berücksichtigung der einschlägigen technischen Richtlinien überprüft sowie an die sich ändernden bzw. erweiternden IT-Strukturen und geänderten Schutzbedürfnisse und Gefährdungen angepasst.

Anlage 2 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

1. Microsoft Ireland Operations Ltd,
   One Microsoft Place, South County Business Park, Leopardstown
   Dublin 18, D18 P521, Ireland

   Betrieb der für CI-Cloud Portal erforderlichen Microsoft Azure Infrastruktur (Server, Load Balancer, File Store, Redis Cache, Firewall, u.A.)

2. Microsoft Corporation
   Attn: Chief Privacy Officer
   1 Microsoft Way
   Redmond, WA 98052, USA

   Betrieb der für CI-Cloud Portal erforderlichen Microsoft Azure Infrastruktur (Server, Load Balancer, File Store, Redis Cache, Firewall, u.A.)