Datenschutzvereinbarung
Wartung und Pflege von IT-Systemen

zwischen

Bitte geben Sie Firmenname mit dazugehöriger Anschrift hier an.

- Auftraggeber -

und

ci solution GmbH

Andreas Stäblein Straße 14

97280 Remlingen

- Auftragnehmer -

Präambel

Zwischen den Parteien besteht ein Vertragsverhältnis über technischen Support für das vom Auftraggeber erworbene Software Produkt der ci solution GmbH.

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

1. Allgemeines

Der Auftragnehmer führt im Auftrag des Auftraggebers technischen Support (z.B. Remotezugriff, telefonischer Support, E-Mail Support) durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis darüber erlangt.

2. Dauer und Beendigung des Auftrags

(1) Der Auftragnehmer führt für den Auftraggeber Leistungen (technischen Support) durch. Zwischen den Parteien besteht diesbezüglich ein Vertragsverhältnis („Hauptvertrag“), das entweder auf individuellen vertraglichen Vereinbarungen, allgemeinen Geschäftsbedingungen oder auf gesetzlichen Regelungen (z.B. BGB) basiert. Diese Vereinbarung beginnt ab Unterzeichnung durch beide Parteien und gilt für die Dauer des jeweiligen Hauptvertrages.

(2) Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

3. Gegenstand des Auftrags

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst nachfolgende Arbeiten und/oder Leistungen. Diese 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.

Der Auftragnehmer ist nicht an personenbezogene Daten des Auftraggebers, seinen Mitarbeitern, Kunden oder Lieferanten interessiert und verarbeitet diese nicht. Im Rahmen des technischen Supports, kann der Auftragnehmer jedoch in Berührung mit personenbezogenen Daten kommen, da Beispielsweise ein Zugriff auf Outlook (E-Mails) oder in das Active Directory erforderlich sind.

Bei Durchführung der oben genannten Arbeiten und Leistungen, demnach nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf folgende Daten/Datenarten hat:

- Benutzerdaten / Personenstammdaten aus dem Active Directory
- Kontaktdaten von Lieferanten und Kunden
- E-Mails, mit den darin enthaltenen Daten

Kreis der davon Betroffenen:

- Mitarbeiter
- generell, Anwender / Benutzer der Netzwerk-Infrastruktur / Domäne des Auftraggebers
- Kunden
- Lieferanten

4. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Wartung und Pflege von IT-Systemen gegenüber dem Auftragnehmer zu erteilen. Weisungen können

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

erfolgen.

(2) 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 für eine optionale Nachweiserbringung in Form von Testaten, von Berichten oder Berichtsauszügen unabhängiger Instanzen oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit anfallen. Kontrollmaßnahmen sind vor ihrer Durchführung hinsichtlich der Art und Weise sowie den zu erwartenden Aufwänden zwischen den Parteien abzustimmen. Die Kosten liegen pro Tag bei pauschal 1280,00 Euro /netto.

(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 Beauftragung von Subunternehmen durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig.

(2) Der Auftragnehmer hat den Subunternehmer 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 Subunternehmer 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. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten nach Art. 37 DSGVO i.V.m. § 38 BDSG (neu) bestellt hat, soweit dieser gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet ist.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Subunternehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(4) Die Verpflichtung des Subunternehmens muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 5 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.

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. Wahrung von Betroffenenrechten

Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

11. 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.

12. 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.

13. 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.

14. 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.
- 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.

15. Zugangskontrolle

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

Getroffene Maßnahmen zur Zugangskontrolle:

- Alle Systeme sind durch Passwort 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.

16. 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.
- Der Zugriff auf die Buchhaltungssoftware ist auf die Geschäftsführung und Buchhaltung 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.

17. 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 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.

18. 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).

19. 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.

20. 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.

21. 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 Telekommunikationsgeheimnis nach § 88 TKG 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.