Vertrag über die Verarbeitung von Daten im Auftrag

zwischen

Klicken oder tippen Sie hier, um Text einzugeben.
Klicken oder tippen Sie hier, um Text einzugeben.
Klicken oder tippen Sie hier, um Text einzugeben.
Klicken oder tippen Sie hier, um Text einzugeben.

- Auftraggeber -

und

KUHN IT GmbH
Schillerstrasse 81
73642 Welzheim

- Auftragnehmer –

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 des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung

nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

7(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. 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. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(5) 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. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

(7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. 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 eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) 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, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu diesem Vertrag angeben.

(2) 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.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

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

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 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. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, 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 seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

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. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

14. 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. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

(2) Er ist mit einer Frist von drei Monaten zum Quartalsende kündbar.

(3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. 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, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(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.

(3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

18. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

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

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

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Erbringung von ASP-Lösung im Kanzleiumfeld

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

☒Personenstammdaten (z.B. Name, Anschrift, Geburtsdatum)
☒ Kommunikationsdaten (z.B. Telefon, E-Mail, Fax)
☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
☒ Gehaltsdaten und Steuerdaten
☒ Kundenhistorie
☐ Besondere Art personenbezogener Daten (rassische/ethnische Herkunft; politische Meinung; religiöse/philosoph. Überzeugung; Gewerkschaftszugehörigkeit; Gesundheitsdaten; Sexualleben) Bitte in diesem Fall den Datenschutzbeauftragten informieren.
☒ Vertragsabrechnungs- und Zahlungsdaten
☐ Daten zu Bank- und Kreditkartenkonten
☐ Planungs- und Steuerungsdaten
☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen
☐ Daten zum Krankenversicherungsstatus (z.B. Krankenkasse, Versichertennummer, Status)
☐ Vorgangsbezogene Daten (z.B. Diagnosen, Zuzahlungspflicht, Unfalldatum)

3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

☒ Kunden des Auftraggebers
☒ Interessenten/Werbekontakte
☒ Beschäftigte
☒ Lieferanten
☒ Handelsvertreter
☒ Ansprechpartner
☒ Beschäftigte von Fremdfirmen
☒ Behörden und sonstige öffentliche Stellen

4. Weisungsberechtigte Personen des Auftraggebers

Hier ggf. Personen benennen oder Passage streichen.

5. Weisungsempfangsberechtigte Personen des Auftragnehmers

Hier ggf. Personen benennen oder Passage streichen.

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:

DATEV eG, 90429 Nürnberg, Paumgartnerstr. 6 - 14	Rechenzentrumsleistungen	Hosting, Fehleranalyse
Citrix Systems UK Ltd, Chalfont Park, Building 3, SL9 OBG, Gerrards Cross, GB	Rechenzentrumsleistungen	Fehleranalyse
Avira GmbH & Co. KG, Kaplaneiweg 1, 88069 Tettnang	Rechenzentrumsleistungen	Fehleranalyse
Kaspersky Labs GmbH Despag-Straße 3 D-85055 Ingolstadt	Rechenzentrumsleistungen	Fehleranalyse
Sophos Technology GmbH (Karlsruhe) Amalienbadstr. 41/ Bau 52 76227 Karlsruhe	Rechenzentrumsleistungen	Fehleranalyse
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Rechenzentrumsleistungen	Fehleranalyse
c-entron software gmbh Liststraße 1 89079 Ulm	Software für Supportleistungen	
REISSWOLF International AG Im Hegen 13 22113 Oststeinbek	Zertifiziertes Entsorgungs-unternehmen für IT-Hardware und Dokumente	Dienstleistungen
LANCOM Systems GmbH Adenauerstrasse 20 / B2 52146 Würselen	Rechenzentrumsleistungen	Fehleranalyse
DRUCK-LOS GmbH Im Schwenkrain 10 70376 Stuttgart	Druckdienstleistungen	Dienstleistungen
TeamViewer GmbH Jahnstr. 30 73037 Göppingen	Fernwartung	

Freie Mitarbeiter der KUHN IT GmbH, die in gleicher Weise auf den Datenschutz verpflichtet worden sind wie deren festangestellte Mitarbeiter:

Anlage 3 -Technische und organisatorische Maßnahmen des Auftragnehmers

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

1 Dokumenteninformation

Die EU-Datenschutzgrundverordnung (DSGVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar.

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind:

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. 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 (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

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

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

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

Um diesen Geboten der Datensicherheit zu genügen, hat die KUHN IT GmbH die nachstehend unter Ziff. 4 ff. beschriebenen Maßnahmen ergriffen.

In diesem Dokument mit aufgenommen sind die jeweils für ihren Anwendungsfall erforderlichen technischen- organisatorischen Maßnahmen der Unterauftragnehmer. Diese sind ebenfalls nach Art. 32 DSGVO sorgfältig ausgewählt und werden laufend überprüft.
Gesetzlich geregelt ist die Datensicherheit in Art. 32 Abs. 1 DSGVO. Die Vorschriften fordern, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.
Für eine automatisierte Verarbeitung (also vor allem per Hard- und Software) nennen die Gesetze (nach DSGVO) verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit und Belastbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
5. Pseudonymisierung und Verschlüsselung

Für nicht-automatisierte Verarbeitungen von personenbezogenen Daten (also ohne Computer) sind die oben genannten Kontrollbereiche nach dem Gesetzeswortlaut nicht direkt anwendbar. Es wird jedoch empfohlen, für einen bestmöglichen Schutz auch in diesen Fällen die Datensicherheit in Anlehnung an die Kontrollbereiche zu organisieren.

All diese Maßnahmen stellen wir in der Folge vor um unseren Informationspflichten aus Art. 32 Abs. 3 lit. c nachzukommen.

2 Versionshistorie

Version	Status	Datum	Verantwortlich	Änderung
1.0	In Kraft	27.04.2018	Kraft/Schairer	Anlage zu § 9 BDSG angepasst auf DSGVO

3 Organisatorisches

Die KUHN IT GMBH hat gemäß Art. 37 DSGVO einen externen Datenschutzbeauftragten in Person von Udo Schairer bestellt. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind schriftlich auf das Datengeheimnis sowie auf die Vertraulichkeit verpflichtet. Der Datenschutzbeauftragte führt regelmäßig Überwachungsaudits sowie fachspezifische Schulungen durch. Die KUHN IT GMBH gewährleistet die schriftliche Dokumentation des aktuellen Datenschutz- Niveaus sowie die schriftlichen Arbeitsanweisungen, Richtlinien und Merkblätter für Mitarbeiter. Zudem sind Verfahren im Bereich Benachrichtigung, Auskunftsersuchen sowie Anliegen zur Berichtigung, Löschung und Sperrung implementiert.

4 Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der KUHN IT GmbH zum Datenschutz gemäß Art. 32 DSGVO betrieben werden.

Die Server, Datenbanken sowie die Datensicherung (Backup) werden bei der KUHN IT GmbH oder beauftragten Dritten in professionellen Rechenzentren betrieben und

gewartet. Die Unterbeauftragten werden sorgfältig ausgewählt und hinsichtlich ihres Sicherheitsbewusstseins und ihrer Fachkompetenz überprüft.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlich werden.

Es wird ausdrücklich darauf hingewiesen, dass die eigentliche Datenverarbeitung auf Servern erfolgt, die im Rechenzentrum der DATEV in Nürnberg/BR Deutschland untergebracht sind. Im Bereich PARTNERasp sind somit die technisch-organisatorischen Maßnahmen der DATEV für das hiesige Auftragsdatenverarbeitungsverhältnis relevant. Sie finden unsere Vereinbarung zur Auftragsdatenverarbeitung mit der DATEV, indem Sie mit dem Internet Explorer oder Microsoft Edge die Webseite www.datev.de/av aufrufen.

1.1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.11 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

#	Maßnahmen
1	Das Verhalten gegenüber Fremdpersonen ist fester Bestandteil der jährlich stattfindenden Datenschutzschulung. Bei dieser handelt es sich um eine Pflichtveranstaltung; ein Fernbleiben ist zu begründen und wird nur bei Vorliegen eines wichtigen Grundes akzeptiert. Die Schlüsselausgabe ist formalisiert und wird protokolliert. Auf die Sorgfaltspflichten im Umgang mit den Zutrittsmedien wird ebenfalls im Rahmen der Datenschutzschulung eingegangen. Fenster und Türen sind grundsätzlich verschlossen zu halten. Auf einschlägige Mittel der Zugangskontrolle wird an dieser Stelle verwiesen. Der unternehmenseigene Serverraum ist grundsätzlich versperrt; der Zutritt ist exklusiv.

4.12 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

#	Maßnahmen
1	Vorgaben zur Komplexität, Länge, Lebensdauer und Historie eines Kennwortes werden durchgesetzt. Der Benutzer wird zudem nach einer bestimmten Anzahl von Falscheingaben automatisch gesperrt. Kennwörter dürfen ferner weder den ganzen noch Teile des Kontonamens des Benutzers beinhalten. Auch die Passwortgrundsätze sind fester Bestandteil der jährlich stattfindenden Datenschutzschulung. Weitere Maßnahmen der Zugangskontrolle: Sämtliche Programme verfügen über eine benutzerbezogene Datenhaltung, die – soweit möglich – an die Windowsanmeldung gekoppelt ist. An- und Abmeldungen werden protokolliert, sofern und insoweit dies seitens des Auftragnehmers technisch umsetzbar und angemessen ist sowie vom jeweiligen Softwarehersteller unterstützt wird. Regeln- und Zugriffsrechte werden ganz allgemein gemäß den Weisungen der Geschäftsleitung/eines Vorgesetzten und differenziert

	vergeben. DATEV Online-Anwendungen werden mittels einer 2-Faktor-Authentifizierung abgesichert. Nutzer werden identifiziert; eine Berechtigungsprüfung wird durchgeführt. Die Benutzerverwaltung ist formalisiert; der Kreis der befugten Nutzer begrenzt. Für das Serversystem gilt: Gescheiterte Zugriffsversuche werden protokolliert; die An- und Abmeldedaten sämtlicher Benutzer werden erfasst (Zeitraum: 180 Tage). Angefertigte Protokolldateien werden in Fällen mit einem konkreten Verdachtsmoment unter Beachtung des Vier-Augen-Prinzips ausgewertet. Wird eine RDG-Funktion verwendet, so ist diese mittels einer auf SSL basierenden Technologie abgesichert. Ferner kommen Viwas und DATEVnet zum Einsatz. Datenbankserver sind gesondert und besonders zugriffsgeschützt. Auf der Betriebssystemebene wird überdies sichergestellt, dass eine mehrfache und gleichzeitige Anmeldung über ein Benutzerkonto ausgeschlossen ist. Ganz allgemein ist eine Clean-Desk-Policy vorgegeben und zu beachten. Der Umgang mit verkörperten Daten ist Bestandteil der jährlich stattfindenden Datenschutzschulung (z. B. Unterverschlussnahme, Entnahme aus dem Laufwerk usw.). Mobile Smartphones werden mittels Active Directory verwaltet.

4.13 Zugriffskontrolle

Maßnahmen die 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.

#	Maßnahmen
1	Zugriffsbefugnisse werden festgelegt und kontrolliert; dabei wird nach Daten, Programmen und Zugriffsart differenziert. Die zugreifenden Nutzer werden identifiziert. Zugriffe sowie Missbrauchsversuche werden auf einer hohen Gliederungsebene protokolliert. Angefertigte Protokolldateien werden in Fällen mit einem konkreten Verdachtsmoment unter Beachtung des Vier-Augen-Prinzips ausgewertet. Darüber hinaus erfolgt eine Authentisierung mittels Passwort und bei Nutzung der DATEV-online-Anwendungen eine 2-Faktor- Authentifizierung. Mobile Smartphones werden mittels Active Directory verwaltet.

4.14 Trennungsgebot

Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

#	Maßnahmen
1	Die Maßnahmen der KUHN IT GmbH zur Trennungskontrolle gewährleisten eine getrennte Verarbeitung der zu unterschiedlichen Zwecken erhobenen Daten. Hierzu erfolgen eine Trennung nach unterschiedlichen Sachgebieten und eine logische Trennung von Daten (unternehmensinterne Daten, Kundendaten, sonstige Daten). Die verantwortlichen Mitarbeiter und deren Handlungsspielräume wurden fest zugeordnet.

1.2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

4.15 Weitergabekontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

#	Maßnahmen
1	Die KUHN IT GmbH ist sich der Tatsache bewusst, dass Wechseldatenträger (z.B. USB-Sticks, externe Festplatten) inventarisiert und verschlüsselt werden müssen. Das Unternehmen bringt die seitens der DATEV angebotene E-Mail-Verschlüsselung zum Einsatz. Die Transportwege der DATEV sind zertifikatsbasiert verschlüsselt. Entsorgungsgut mit schutzwürdigem Inhalt wird physikalisch vernichtet. Dabei wird auf eine ausreichende/angemessene Sicherheitsstufe geachtet, die sich nicht zuletzt an der Schutzklasse des jeweiligen Datenträgers orientiert.

4.16 Eingabekontrolle

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

#	Maßnahmen
1	Rechteänderungsprotokolle werden geführt, sofern und insoweit dies seitens des Auftragnehmers technisch umsetzbar und angemessen ist sowie vom jeweiligen Softwarehersteller unterstützt wird. Diese Protokolldaten werden gegen Verlust oder Veränderung geschützt, sofern und insoweit dies seitens des Auftragnehmers technisch umsetzbar und angemessen ist sowie vom jeweiligen Softwarehersteller unterstützt wird. Gescheiterte Zugriffsversuche werden protokolliert; die An- und Abmeldedaten sämtlicher Benutzer werden erfasst (Zeitraum: 180 Tage), sofern und insoweit dies seitens des Auftragnehmers jeweils technisch realisierbar und angemessen ist sowie vom jeweiligen Softwarehersteller unterstützt wird. Gemäß dem Datenschutzhandbuch der KUHN IT GmbH wird bei einer Auswertung dieser Protokolle nach dem Vier-Augen-Prinzip verfahren.

1.3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Maßnahmen die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

#	Maßnahmen
1	Die Datensicherung umfasst die von der KUHN IT GmbH genutzten Daten-Server und die dort abgelegten Daten. Zudem werden zusätzliche Server erfasst, die zum Hosting weiterer Funktionen (z.B. CTI) notwendig sind. Die Datensicherung wird 3x täglich zu festen Zeiten durchgeführt. Das Zeitfenster der Datensicherung kann je nach Veränderungen der Daten oder Veränderungen im System bzw. der Systemumgebung und dem vorhandenen Datenvolumen variieren. Aufgrund einer Lastverteilung kann eine Aussage, wann die Datensicherung

	im Einzelnen beginnt und endet, im Vorfeld nicht getroffen werden. Art und Weise sowie technische Realisierung der Datensicherung obliegen der KUHN IT GmbH. Es werden 14 tägliche Sicherungspunkte vorgehalten (entspricht 14 Tagen). Die Daten können im Rahmen der Datenrücksicherung auf jeden Endstand vor Beginn einer Sicherung der vorangegangenen 42 Sicherungspunkte wiederhergestellt werden. Es wird eine Erfolgskontrolle der Datensicherung durchgeführt; eventuell auftretende Fehler werden behoben.

1.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d DSGVO)

4.17 Datenschutz-Management

Wir nutzen ein Datenschutzmanagementsystem (DSMS), in dem alle Maßnahmen, Verfahren, Tätigkeiten etc. im Bereich Datenschutz abgebildet werden. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen und beinhaltet darüber hinaus einen Maßnahmenplan zur rechtskonformen Umsetzung der EU-Datenschutzgrundverordnung (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO).

4.18 Incident-Response-Management

Ein Helpdesk System (Ticketsystem) zur unverzüglichen Meldung aller Arten von Incidents an die IT ist implementiert. In der Anwenderrichtlinie sind Prozesse und Meldewege mit Vorgehen und Verantwortlichen dokumentiert. Zudem kommen Intrusion-Detection-Systeme zur Anwendung.

4.19 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden.

4.20 Auftragskontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Sollte die KUHN IT GMBH bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der. Zudem stellt die KUHN IT GMBH folgende Voraussetzungen für ein Unterauftragsverhältnis sicher:

#	Maßnahmen
1	Die zur Verarbeitung eingereichten Daten werden entsprechend den gesetzlichen Vorschriften nur im Rahmen der Weisungen des jeweiligen Auftraggebers verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben. Der Weisungsrahmen ist insbesondere durch den schriftlich geschlossenen Vertrag zur Datenverarbeitung im Auftrag eindeutig vorgegeben. Gleiches gilt für auftragsbezogene Auskünfte: sie werden ausschließlich an den Auftraggeber oder im Rahmen seiner Weisungen erteilt. Eine flächendeckende Auftragskontrolle ist eingerichtet. Die konkreten Maßnahmen zur Auftragskontrolle beinhalten eine einheitliche und

	eindeutige Vertragsgestaltung, eine formalisierte Auftragserteilung mit Auftragsformular und die Kontrolle der Vertragsausführung. Die Auftragnehmer werden sorgfältig entsprechend den dortigen Datenschutz- und Datensicherheitsstandards ausgewählt.

1.5. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Entsprechende Verschlüsselungssysteme für Datenträger und mobile Endgeräte sind implementiert (Bitlocker-Verschlüsselung). Verschlüsselungstechnologien bei der Übermittlung von Daten kommen ebenfalls zum Einsatz. Eine Richtlinie zum Umgang mit (mobilen) Datenträgern kommt zur Anwendung. Auch restriktive Zugriffsrechte beim Zugriff auf Server, Datenbanken etc. werden angewandt.

1.6. Externer Datenschutzbeauftragter

Externer Datenschutzbeauftragter gemäß. Art. 37 Datenschutzgrundverordnung (DSGVO):

Udo Schairer
Tennhöfleweg 21
73553 Alfdorf

E-Mail: datenschutz@kuhnit.de