Der Vertrag ist bereits digital unterzeichnet und in dieser Form gültig. Bitte drucken Sie diesen aus, unterzeichnen als „Auftraggeber“ und senden uns einen Scan / ein hochauflösendes Foto per E-Mail an info@akentas.de zurück. Erst dann gilt der Vertrag als abgeschlossen.

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

- nachfolgend **Auftraggeber** genannt -

und

Akentas GmbH
Im Winkel 6
78333 Stockach

- nachfolgend **Auftragnehmer** genannt -

1. Allgemeines

1.1. 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.

1.2. 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

3.1. 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.

3.2. 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.

3.3. 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.

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

3.5. 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.

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

3.7. 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

4.1. 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.

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

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

4.4. 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.

4.5. 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.

4.6. 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.

4.7. 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.

4.8. 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

5.1. 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.

5.2. 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

6.1. 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.

6.2. 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.

6.3. 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

7.1. 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.

7.2. 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.

7.3. 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

8.1. 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.

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

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

8.4. 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.

8.5. 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

9.1. 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.

9.2. 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.

9.3. 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 Datenschutzbeauftragte zu benennen.

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

9.5. 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.

9.6. 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.

9.7. 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

10.1. 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.

10.2. 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.

10.3. Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

11.1. 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.

11.2. 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.

11.3. 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

12.1. 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.

12.2. 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

14.1. 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.

14.2. 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.

14.3. 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

15.1. Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

15.2. Er ist mit einer Frist von drei Monaten zum Quartalsende kündbar.

15.3. 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

16.1. 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.

16.2. 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.

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

18.1. 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.

18.2. Für Nebenabreden ist die Schriftform erforderlich.

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

_____, den _____

Wahlwies, den 25.05.2018

_____

- Auftragnehmer -

_____

- Auftraggeber -, Miro Grenda (CEO)

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftragnehmer ermöglicht seinen Kunden die Nutzung eines Content-Management-Systems zum Anlegen und Verwalten von Webprojekten (webXsite®), wobei die Webprojekte für den Kunden auf einem Server gehostet werden (nachfolgend zusammenfassend „Service“). Der bereitgestellte Service erlaubt es den Nutzern, selbständig das Design der eigenen Website anzupassen und eigene Inhalte einzustellen. Der Gegenstand des Auftrags ergibt sich im Übrigen aus dem zwischen den Parteien geschlossenen Hauptvertragsverhältnis. Dieses beruht auf den AGB von webXsite, die wirksam in das Vertragsverhältnis zwischen den Parteien einbezogen wurden. Dieser Vertrag zur Auftragsverarbeitung gilt ergänzend zu den AGB von webXsite (https://www.webxsite.com/agb.aspx).

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

- Technische Umsetzung des Webprojektes (z.B. auf Basis des im Vorfeld übermittelten Screendesigns und/oder einem Anforderungskatalog)
- Technisches Betreiben, Anpassen und Bereitstellen des Service
- Bereitstellung der einzelnen Websites sowie First-Level-Support

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Personenstammdaten (z.B. Name, Anschrift)
- Kommunikationsdaten (z.B. Telefonnummer, Email Adresse)
- Vertragsstammdaten (z.B. Produktbezeichnung, Preise)
- Vertragsabrechnungs- und Zahlungsdaten
- Kundenhistorie

3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Kunden des Auftraggebers
- Interessenten bzw. Besucher der Website des Auftraggebers
- Mitarbeiter des Auftraggebers

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“):

Unternehmen/Dienst	Leistung/Verwendung
centron GmbH, Heganger 29, 96103 Hallstadt www.centron.de/data-protection/	Bereitstellung von Webhosting-Dienstleistungen (Registrierung und Verwaltung von Domains, Email, Webserver/Webspace, SSL Zertifikate)
DomainFactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning - www.df.eu/de/datenschutz/	Bereitstellung von Webhosting-Dienstleistungen (Registrierung und Verwaltung von Domains, Email, Webserver/Webspace, SSL Zertifikate)
Newsletter2Go GmbH, Köpenicker Str. 126, 10179 Berlin www.newsletter2go.de/datenschutz-grundverordnung	Verwendung von Adressdaten des Auftraggebers zur Versendung von Newslettern per Email
Google LLC., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA www.google.de/intl/de/policies/privacy	Nutzung diverser Dienste von Google wie Google Maps, Google Fonts, Google Analytics auf eigenen Websites und innerhalb unseres Services
PayPal (Europe) S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, 2449 Luxembourg www.paypal.com/de/webapps/mpp/ua/privacy-full	Nutzung von Paypal für Zahlungsabwicklung
Dropbox International Unlimited Company, One Park Place, Floor 5, Upper Hatch Street, Dublin 2, Irland - www.dropbox.com/de/security/GDPR	Nutzung von Dropbox Business für Datenablage
Youtube Ein Produkt der Google LLC., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA www.google.de/intl/de/policies/privacy	Einbettungsfunktion zur Anzeige und Wiedergabe von Videos des Anbieters YouTube auf eigenen Websites und innerhalb unseres Services
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA www.microsoft.com/en-us/Licensing/product-licensing/products.aspx#OST	Nutzung diverser Dienste von Microsoft wie Office365 für Email, OneDrive und OneNote für Datenablage, Skype und Skype Business für Kommunikation, Azure für Bereitstellung von eigenen Diensten und als Dateiablage
Github, 88 Colin P Kelly Jr St, San Francisco, CA 94107, USA help.github.com/articles/github-privacy-statement/	Intern verwendeter Online-Dienst für die Code-Verwaltung
Trello Atlassian, 55 Broadway Floot 17 & 25, New York, NY 10006 USA - trello.com/privacy	Intern verwendeter Online-Dienst für Aufgabenplanung
easybill GmbH, Düsselstr. 21, 41564 Kaarst www.easybill.de/privacy	Intern verwendeter Online-Dienst für die Erstellung von Rechnungen, Angeboten, Lieferscheinen und ähnlichen Dokumenten
Evernote Corporation, 305 Walnut Street, Redwood City, CA 94063, USA - evernote.com/intl/de/privacy	Intern verwendeter Online-Dienst für Notizen, Dokumente und Fotos

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. Vertraulichkeit

Zutrittskontrolle

Unbefugten ist der Zutritt zu Daten-verarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

In den Büroräumen des Auftragnehmers werden in der Regel keine personenbezogenen Daten für den Auftraggeber gespeichert. Alle auftragsbezogen genutzten IT-Systeme befinden sich in Rechenzentren die der Auftragnehmer nutzt.

Speicherung der Daten Rechenzentren, dort:

- Zugangskontrollsystem
  - Türsicherung im Bürogebäude (elektrische Türöffner mit Zugriffsprotokollierung sowie protokollierte Schlüsselvergabe gemäß Schlüsselmanagement).
  - Zusätzliche biometrische Zugangssicherung zum Rechenzentrum und elektronische Türsicherung zwecks zweistufiger Zutrittskontrolle.
- Einrichtung von Schutzzonen und Festlegung von Zutrittsregeln
- Besucherregelung
  - Protokollierung sämtlicher Besucher
  - Besuche und Lieferanten unterliegen in Abhängigkeit der Schutzzone einer durchgängigen Aufsicht.
- Rundum Videoüberwachung des Gebäude-Außenbereichs mit Sabotageerkennung und Aufzeichnung. Lückenlose Videoüberwachung des Rechenzentrum-Innenbereichs.
- Einbruchmeldeanlage mit Aufschaltung des Sicherheitsdienstes

Zugangskontrolle

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

- Erteilung von Berechtigungen durch Leitung der Technik und Geschäftsführung
- Berechtigte erhalten individuelle Nutzer-IDs die beim Zugriff auf die Systeme zur Authentifizierung eingesetzt werden müssen (jeder Zugriff erfordert eine Passworteingabe)
- Sichere Passwörter (u.a. Sonderzeichen, Mindestlänge) deren Weitergabe untersagt ist
- Nach Beendigung der Beschäftigung wird die individuelle Nutzer-ID deaktiviert
- Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden

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.

- Die Passwortvergabe erfolgt ausschließlich durch berechtigtes Personal an vom Auftraggeber benannte Personen
- Die Berechtigung zur Datenverarbeitung personenbezogener Daten werden durch das Active-Directory gesteuert und protokolliert
- Es ist Sache des Auftraggebers dafür Sorge zu tragen das ihm überlassene Passwort zum System des Auftragnehmers nur an geeignete/berechtigte Personen weiter zu geben und diesen Zugriff zu gewähren (jeder der das Passwort kennt, kann Änderungen am Webprojekt vornehmen)

Trennung

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

- Es wird ausschließlich Software verwendet, die eine Mandantenfähigkeit bereitstellt
- Die Daten können aufgrund der Art ihrer Speicherung getrennt voneinander verarbeitet werden
- Trennung der verarbeitenden Systeme
- Trennung der Systeme in Produktiv- und Testumgebung
- Kunden haben gegenseitig keinen Zugriff auf andere Kundensysteme
- Es ist Sache des Auftraggebers dafür Sorge zu tragen personenbezogene Daten auf dem ihm überlassenen System und den Webprojekten zu trennen

2. Integrität

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.

- Es ist Sache des Auftraggebers ggf. personenbezogene Daten in das ihm überlassene System (Webprojekt) einzugeben und zu pflegen und dafür Sorge zu tragen nur geeignete Dritte einzusetzen. Der Auftragnehmer wird grundsätzlich nicht auf diese Daten zugreifen bzw. Daten eingeben, verändern oder löschen
- Das Verarbeiten von personenbezogenen Daten erfolgt somit grundsätzlich durch den Auftraggeber, so dass durch den Auftragsverantwortlichen nicht nachträglich überprüft werden und festgestellt werden kann, welche personenbezogenen Daten der Kunde zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert hat
- Nur im Rahmen seiner Tätigkeiten nach zusätzlicher Weisung, die in Textform und außerhalb des Webprojekt-Administrationsbereichs stattfindet, dokumentiert der Auftragnehmer diese Eingaben und Veränderungen in angemessener Weise
- Muss der Auftragnehmer aus gesetzlichen Gründen Informationen entfernen oder den Zugang zu ihnen sperren, wird die Sperrungen bzw. die Entfernung in angemessener Weise dokumentiert

Weitergabekontrolle

Es ist 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.

- Eine Weitergabe von Daten des Auftraggebers findet grundsätzlich nicht statt. Ausgenommen hiervon sind Fälle, in denen der Auftragnehmer aufgrund gesetzlicher Regelungen oder richterlichen Anordnungen zur Herausgabe von Daten verpflichtet ist
- Eine Weitergabe von Daten, die auf dem System des Auftragnehmers im Auftrag des Auftraggebers gespeichert werden, erfolgt ansonsten nur im Zusammenhang mit dem vom Auftraggeber vorgesehenen Betrieb seiner Internetpräsenz (Aufruf der Internetseiten durch Besucher der Internetseite) im jeweils technisch erforderlichen Umfang
- Die Gewährleistung der Vertraulichkeit der Übermittlung von personenbezogenen Daten wird durch SSL/TSL-Verschlüsselungen über das System des Auftragnehmers gewährleistet
- Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert
- Soweit möglich werden Daten verschlüsselt an Empfänger übertragen
- Mitarbeiter des Auftragnehmers werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden

3. Verfügbarkeit und Belastbarkeit

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

- Die vom Auftragnehmer genutzten Rechenzentren verfügen über Unterbrechungsfreie Stromversorgung (USV), Notstrom-Dieselanlage, redundante Klimaversorgung, Brandfrüherkennungsanlage – die Mitarbeiter werden regelmäßig zum Thema Brandbekämpfung geschult
- RAID (redundante Datenschreibung auf Festplatten)
- Sicherungskopien werden in Form von Backups gemäß Backupkonzept erstellt
    - Vollsicherung alle 4 Wochen, Aufbewahrungszeit: 5 Wochen
    - Sicherung Änderungen zur Vollsicherung jede Woche, Aufbewahrungszeit: 2 Wochen
    - Sicherung Änderungen zur letzten wtl. Sicherung jeden Tag, Aufbewahrungszeit: 1 Woche
- Dateiformat: binär, proprietär verschlüsselt
- Aufbewahrungsort ist ein Storagesystem im Rechenzentrum
- Regelmäßige Prüfung der Backups auf Funktionalität
- Umsetzung von Disaster und Recovery Konzept, Notfallkonzept und Wiederanlaufplan

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Mitarbeiter des Auftragnehmers werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag sowie im Hinblick auf das Weisungsrecht des Auftraggebers.

Jeder Mitarbeiter wird spätestens am ersten Tag zu Beginn seiner Tätigkeit schriftlich zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO verpflichtet. Ohne Vorliegen dieser Erklärung erhält der Mitarbeiter keinen Zugriff auf personenbezogene Daten.