Vereinbarung über die Verarbeitung von Daten im Auftrag

zwischen

MUSTER

- Verantwortlicher -

und

AixConcept GmbH
vertreten durch den/die Geschäftsführer
Wallonischer Ring 37
52222 Stolberg (Rhld.)

- Auftragnehmer / Auftragsverarbeiter -

1. Allgemeines

(1) Zwischen dem Verantwortlichen gemäß Art. 4 Nr. 7 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) und dem Auftragsverarbeiter kommt eine Verarbeitung von Daten im Auftrag im Sinne der Art. 4 Nr. 8 und Art. 28 DSGVO zustande.

Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten.

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

2. Gegenstand des Auftrags

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

3. Rechte und Pflichten des Verantwortlichen

(1) Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Verantwortlichen darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

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

(3) Der Verantwortliche 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) Der Verantwortliche 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 Verantwortlichen ändern, wird der Verantwortliche dies dem Auftragnehmer in Textform mitteilen.

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

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Verantwortlichen geltenden gesetzlichen Meldepflicht besteht, ist der Verantwortliche 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 Verantwortlichen erteilten schriftlich ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen 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 Verantwortlichen. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Verantwortliche dieser schriftlich zugestimmt hat.

(2) Die Verarbeitung der Daten findet vorwiegend in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Die Verarbeitung personenbezogener Daten in ein Drittland darf nur erfolgen, wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind.

Entsprechend wird das angemessene Schutzniveau entweder festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO), hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b) i. V. m. 47 DSGVO), hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c) und d) DSGVO), hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e) i. V. m. 40 DSGVO), hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f) i. V. m. 42 DSGVO) oder wird hergestellt durch sonstige Maßnahmen gemäß Art. 46 Abs. 2 lit. a), Abs. 3 lit. a) und b) DSGVO).

(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 Verantwortlichen 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 Verantwortlichen abstimmen.

(5) Der Auftragnehmer wird den Verantwortlichen unverzüglich darüber informieren, wenn eine vom Verantwortlichen erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Verantwortlichen 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) Der Auftragnehmer wird die Daten, die er im Auftrag für den Verantwortlichen verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(7) Der Auftragnehmer kann dem Verantwortlichen die Person(en) benennen, die zum Empfang von Weisungen des Verantwortlichen 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 Verantwortlichen 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.

Auf Anfrage werden dem Verantwortlichen die Kontaktdaten des benannten Datenschutzbeauftragten mitgeteilt.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Verantwortlichen jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Verantwortlichen, 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 Verantwortlichen verarbeitet.

(2) Ferner wird der Auftragnehmer den Verantwortlichen 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 Verantwortlichen erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Verantwortlichen 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 Verantwortlichen bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Verantwortlichen insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Verantwortlichen verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Verantwortlichen 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 Verantwortlichen 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 Verantwortlichen mit. Er hat dem Verantwortlichen die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Verantwortlichen 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 Verantwortliche 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 Verantwortlichen durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(1a) Der Verantwortliche setzt für die Kontrollen im Sinne des Absatzes 1 entweder eigenes Personal oder externe Dienstleister ein, welche nicht gleichzeitig für Mitbewerber des Auftragnehmers tätig sind.

(2) Der Auftragnehmer ist dem Verantwortlichen gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle im Sinne des Absatzes 1 erforderlich ist.

(3) Der Verantwortliche kann eine Einsichtnahme in die vom Auftragnehmer für den Verantwortlichen verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

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

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Verantwortlichen in Textform zulässig. Der Auftragnehmer stimmt der Nutzung der in **Anlage 2** genannten Unterauftragsverhältnisse explizit zu.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Verantwortlichen 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 Verantwortlichen 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 Verantwortlichen 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 Verantwortlichen 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 Verantwortlichen und Auftragnehmer festgelegt sind. Dem Verantwortlichen ist der Vertrag zur Verarbeitung von Daten im Auftrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Verantwortlichen und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Verantwortlichen 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 Verantwortlichen 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 Verantwortlichen genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Verantwortlichen verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Verantwortlichen 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 Verantwortlichen obliegen. Der Verantwortlichen 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 Verantwortlichen informiert hat.

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

11. Wahrung von Betroffenenrechten

(1) Der Verantwortliche ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Verantwortlichen 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 Verantwortlichen 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 Verantwortlichen erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Verantwortlichen treffen. Der Auftragnehmer wird den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

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. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Verantwortlichen 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 Verantwortlichen 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 Verantwortlichen umgesetzt werden. Der Verantwortliche kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Ersetzend zu den Kontrollbefugnissen des Absatzes 8 kann der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, z. B. auch erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Datenschutzbeauftragter) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001).

(4) 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 Verantwortlichen informieren.

14. 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 durch den Verantwortlichen kündbar.

(3) Der Verantwortliche 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 Verantwortlichen nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Verantwortlichen oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

15. 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 Verantwortlichen 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.

(2) Der Verantwortliche 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 Verantwortlichen angekündigt werden.

16. 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.

17. Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Verantwortlichen 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.

_____,	_____	Stolberg	, _____
Ort	Datum	Ort	Datum
_____		_____	
- Verantwortlicher -		- Auftragnehmer -	

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand sowie Art und Zweck der Verarbeitung

Die Verarbeitung von Daten des Verantwortlichen durch den Auftragnehmer umfassen folgende Arbeiten und/oder Leistungen:

Gegenstand der Verarbeitung ist die Bereitstellung des Cloud Service „MNSpro Cloud“ einschließlich der zugehörigen Wartungs-, Pflege- und Supportleistungen durch AixConcept für den Kunden.

Die Verarbeitung der Daten erfolgt auch hinsichtlich der Einholung von Einwilligungen bei den Betroffenen, der Anlage von Benutzerkonten für MNSpro Cloud, und der damit verbunden Anlage eines Cloud-Kontos für Office 365, wozu Vorname, Name, E-Mailadresse an Microsoft Dienste (Office 365 Plattform) übermittelt werden.

Die Datenverarbeitung innerhalb der Office 365 Plattform wird vertraglich zwischen dem Auftraggeber/Verantwortlichen und Microsoft Ireland Operations, Ltd. geregelt und ist nicht Bestandteil dieser Auftragsverarbeitung.

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten des Verantwortlichen ist nicht Zweck des Wartungsvertrags, kann aber zu dessen Erfüllung notwendig werden.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Foto
- Anzeigename
- Familienname
- Vorname
- Externe ID
- Klasse
- Kurse
- Kursjahr bzw. Schuljahr
- E-Mailadresse
- Technische Protokolldaten
- Stundenplan
- Benutzername
- Personenrolle
- Person
- Benutzergruppe

- Benutzerzugang (aktiv, gesperrt)
- Sprache
- E-Mailadresse
- Letzte Anmeldung
- OTP Schlüssel
- Office 365 Tenant ID
- Profileinstellungen
- SchILD-ID
- Passwort (verschlüsselt)/Anmeldename

Bei Verwendung des elektronischen Klassenbuchs

- Abwesenheiten
- Klassenbucheinträge
- Noten
- Befreiungen
- Klassendienste
- Attestpflicht
- Volljährigkeit
- Geburtsdatum
- Protokolldaten
- Informationen innerhalb von Support-Tickets

Bei Verwendung des Elternportals

- Eltern (Vorname, Name)
- Wohnadresse
- Straße, PLZ, Ort
- Telefonnummern
- Mobil, Festnetz
- Weitere Notfallkontakte
- Nachrichten
- (Elternbrief etc.)

Bei Verwendung der Unterrichtszentrale

- Rechnername
- IP-Adresse

Bei Verwendung des Einwilligungsportals

- IP-Adresse zum Zeitpunkt der Einwilligung / des Widerrufs der Einwilligung
- Name des Schülers und/oder dessen Vertreter
- E-Mailadresse des Schülers oder dessen Vertreter
- Mobilfunknummer des Schülers oder dessen Vertreter
- Datum der Einwilligung / des Widerrufs der Einwilligung

Zusätzlich bei Lehrkräften / nicht-unterrichtenden Personal:

- unterrichtete Fächer/Kurse
- unterrichtete Klassen
- dienstliche Telefonnummer
- Gruppenzugehörigkeit (z. B. Fachschaft)
- Protokollierung der Nutzung (kurzfristige Aufbewahrung)

3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Alle Nutzer von MNSpro Cloud
  Personen, deren Daten in MNSpro Cloud verarbeitet werden, u. A.
  - Schülerinnen und Schüler sowie deren Erziehungsberechtigte
  - Lehrkräfte
  - Sonstige Beschäftigte des Verantwortlichen

4. Weisungsberechtigte Personen des Verantwortlichen

BITTE PERSONEN BENNENEN

5. Weisungsempfangsberechtigte Personen des Auftragnehmers

Dr. Guido Moritz, Geschäftsführer

Scott MacKendrick, Geschäftsführer

Stefan Winandy, Vice President Operations

Sebastian Fillinger, Vice President Research & Development

Anlage 2 - Unterauftragnehmer

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

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Unterauftragnehmer	**Art der Leistung**
TeamViewer GmbH Geschäftsführer Oliver Steil Jahnstr. 30 73037 Göppingen Deutschland +49 7161 60692 50 contact@teamviewer.com	Nutzung eines Tools für den Remote-Support.
Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521	Nutzung von unterstützenden Diensten im Rahmen der Wartung und des Betriebs der MNSpro Cloud Plattform zudem Mailversand von Support-Tickets über Office 365. Eigenständige AVV zwischen Ihnen und Microsoft notwendig zur Bereitstellung der IT-Plattform, auf der MNSpro Cloud betrieben wird (siehe Anlage 1, Punkt 1).

Anlage 3
Technische und organisatorische Maßnahmen des Auftragnehmers

Vertraulichkeit
(Art. 32 (1) b) DSGVO)

Geeignete technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit werden, unter Berücksichtigung des Stands der Technik, der Art, des Umfangs, der Umstände, der Zwecke der Verarbeitung, der Implementierungskosten und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen getroffen. Hiermit wird ein dem Risiko angemessenes Schutzniveau gewährleistet.

Zutrittskontrolle

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

Objektsicherung:

- Zutrittssicherung durch mechanische Schließanlage am Gebäude und mechanische Schließanlage im Serverraum.
- Beauftragter Wachdienst (ab Neubau, Wallonischer Ring, Stolberg)

Sicherheitsbereiche:

- Der Serverraum ist ein eigener abgesicherter Bereich
- Weitere Sicherheitsbereiche wurden erstellt und räumlich voneinander getrennt: wie z.B. Innendienst, Schulungszentrum, Buchhaltung, Geschäftsführung usw.

Art der Zutrittskontrolle:

- Mechanische Türsicherungen sind verbaut;
- Schlüssel- und Schließordnung inkl. revisionsfähige Schlüsselliste
- Kontrollgänge nach Ende der Bürozeiten;

Regelungen der Zutrittsberechtigungen:

- Die Zutrittsberechtigungen sind restriktiv ausgestaltet;
- Festlegung befugter Personen mit Bezug auf Sicherheitszonen (z. B. Serverraum, Buchhaltung);
- Besucher müssen sich am Empfang anmelden und werden abgeholt und begleitet;
- Regelungen für das Ausscheiden von Mitarbeitern oder den internen Stellen;
- Regelungen / Folgemaßnahmen bei Verlust von Ausweisen, Schlüsseln usw.;
- Anmeldung und Begleitung von Besuchern und Externen;
- Aufsicht des Wartungs-, Reparatur- und Reinigungspersonals im Serverraum.

Zugangskontrolle:

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

Regelung der Zugangsberechtigungen

- Fixierte Regelungen für die Vergabe von Zugangsberechtigungen getroffen;
- Vergabe erfolgt unter Wahrung des Need-to-know-Prinzips;
- Zugangsberechtigte weisen sich durch Benutzernamen und Passwort aus;
- Regelungen für die Verwendung von Passwörtern, deren Länge, Komplexität und Aufbewahrung;
- Passwörter von Administratoren unterliegen höheren Anforderungen an Komplexität;
- Regelungen für das Deaktivieren nicht benötigter Accounts;
- Regelungen für die Sperrung des Rechners beim Entfernen vom Gerät auch bei kurzer Abwesenheit;
- Regelungen für das Ausscheiden bzw. den Stellenwechsel von Berechtigten;
- Begrenzung der Anmeldeversuche;
- Der Zugang zu den Kundensystemen ist individuell passwortgeschützt;
- Die Zugangsdaten sind nur den zuständigen Mitarbeitern bekannt.

Zusätzliche Maßnahmen beim Fernzugang

- Regelungen für die Benutzung des Anschlusses;
- Netzzugangssicherung durch Hard- und Softwaremaßnahmen.

Protokollierung von Zugängen

- Protokollierung fehlgeschlagener Zugangsversuch;
- Protokollierung der Remotezugänge am (SSL) VPN-Gateway;
- Protokollierung der Vergabe / Änderung von Zugangsberechtigungen.

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.

Berechtigungskonzept

- Berechtigungen werden ausschließlich nach vorheriger Genehmigung gewährt;
- Der Zugriff auf alle Systeme mit personenbezogenen oder sonstigen, schützenswerten Daten ist nur berechtigten Mitarbeitern freigeschaltet und wird über individuelle Passwörter geschützt;
- Nur Supportmitarbeiter und Domainadministratoren haben administrativen Zugang auf das beim Kunden installierte System;
- Die Mitarbeiter sind darüber unterrichtet, auf welche Daten sie regelmäßig Zugriff nehmen dürfen und wurden auf das Datengeheimnis verpflichtet.

Zugriffsschutz

- Trennung von Test und Produktivumgebung;
- Kritische Dienste unterliegen einem Monitoring;
- Verwendung nur freigegebener Hard- und Software;
- Einsatz von Verschlüsselungsroutinen sowie die Möglichkeit zur Dateiverschlüsselung;
- Sichere Löschung von personenbezogenen Informationen nach Wegfall der Rechtsgrundlage.

Aufbewahrung bei Verwendung von Datenträgern

- Aufbewahrung von Datenträgern ist geregelt (sichere Orte);
- Sichere Löschung/Vernichtung von Datenträgern ist gewährleistet;
- Keine Reparatur von Datenträgern, sondern grundsätzlich Entsorgung mit Bestätigung der datenrechtlichen Vernichtung mit Entsorgungsnachweis.

Protokollierung von Zugriffen

- Protokollierung von Netzzugriffen bei administrativen Zugriffen / Aktivitäten sollten (Systemüberwachung).

Trennungskontrolle:

Es ist zu gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.

- Eine logische Mandantentrennung (auch Wartungs-Tickets) findet bei den davon betroffenen Verarbeitungen statt.
- Im Entwicklungs- und Testsystem werden nur Testdaten verarbeitet.

Pseudonymisierung:

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne weitere Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen den entsprechenden technischen und organisatorischen Maßnahmen.

- Pseudonymisierung wird zum jetzigen Zeitpunkt nicht verwendet und wird nach Beauftragung vom Auftragnehmer weisungsgebunden im Einzelfall realisiert

Integrität
(Art. 32 (1) b) DSGVO)

Die Richtigkeit der verarbeiteten personenbezogenen Daten ist zu gewährleisten. Unzulässige Änderungen müssen identifiziert und korrigiert werden können

Weitergabekontrolle:

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

<u>Regelung der elektronischen Übertragung</u>

- Bereitstellung verschiedener Möglichkeiten, um Daten verschlüsselt zu übertragen:
  - SSL-verschlüsselte Datenaustauschplattform;
  - Einrichtung und Nutzung von TLS (zwingend) bei eMail.
- Keine Nutzung unverschlüsselter Übertragungsverfahren für personenbezogene, schützenswerte Daten.

<u>Regelung bei der Speicherung auf Wechseldatenträgern</u>

- Eine Speicherung von personenbezogenen Daten auf Wechseldatenträgern ist grundsätzlich nicht vorgesehen;
- Im Ausnahmefall werden ausschließlich verschlüsselte mobile Datenträger (bei personenbezogenen Daten) verwendet.

<u>Regelungen des Transports von Datenträgern</u>

- Datenträger in mobilen Rechnern sind verschlüsselt;
- Datenträger mit personenbezogen Daten werden verschlüsselt.

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.

- Aktivitäten im Ticketsystem werden namentlich und nicht durch Support-Personal veränderbar und nachweisbar protokolliert;
- Zuständigkeiten für Dateneingabe, einschließlich Vertretungsregelungen sind durch Berechtigungskonzept und Berechtigungsvergabe festgelegt.

Verfügbarkeit und Belastbarkeit der Systeme
(Art. 32 (1) c) DSGVO)

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

Erstellung und Verwahrung von Sicherheitskopien:

- Dokumentiertes Datensicherungskonzept;
- Kontrollierte und regelmäßige Sicherung der Dateien und Datenbanken;
- Tests der Datensicherung werden durchgeführt und dokumentiert;
- Datensicherung ist geschützt vor unberechtigten Zutritt, Zugang und Zugriff;
- Datensicherungsträger werden vor Diebstahl und Zerstörung sicher an besonders geschützten Orten gelagert.

Gewährleistung des laufenden Betriebes:

Der laufende Betrieb ist durch technische und organisatorische Maßnahmen sichergestellt
<u>Stromversorgung/Klimatisierung:</u>

- Wartungsvertrag zur Klimatisierung abgeschlossen.

Unterbrechungsfreie Stromversorgung:

- USV vorgeschaltet für Serversysteme;
- Ordnungsgemäßes Herunterfahren / Funktionsfähigkeit wird durch regelmäßige Tests sichergestellt.

Brandschutz:

- Auf Brandschutz wird geachtet.

Anbindung Internet:

- Redundante Internetanbindung unterschiedlicher Anbieter und Technologien;
- 24/7 Notfall Support bei Internetanbietern.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 (1) d) DSGVO)

Die umfangreichen Pflichten und Anforderungen der EU-DS-GVO erfordern eine ganzheitliche Strategie nach einem strukturierten Ansatz und ein entsprechendes Managementsystem. Alle Elemente, die für die Sicherstellung des Datenschutzes erforderlich sind, unterliegen der systematischen Koordination des Datenschutz-Managements.

Elemente des Datenschutz-Managementsystems:

- Es wurde beim Auftragsverarbeiter ein Datenschutzbeauftragter benannt.
  Er ist erreichbar unter datenschutz@aixconcept.de.
  Weitere Kontaktdaten werden auf Anfrage mitgeteilt.
- Im Rahmen von regelmäßigen, internen Audits und Überprüfungen wird sichergestellt, dass die datenschutzrechtlichen Anforderungen laufend umgesetzt werden.
- Datenschutzrelevante Richtlinien und Arbeitsanweisungen werden verkündet und die Einhaltung kontrolliert.
- Etablierte Prozesse sehen die Einbindung des Datenschutzbeauftragten vor.
- Mitarbeiter sind entsprechend geschult.
- Meldestellen und Meldewege für Datenschutz- und Sicherheitsvorfälle sowie Auskunftsanfragen sind definiert.
- Gewonnene Erfahrungswerte fließen in die weitere Verbesserung der Prozesse ein.

Auftragskontrolle

- Für alle Auftragsverarbeitungen werden Verträge geschlossen.
- Alle Auftragsverarbeiter müssen vorab Leistungsbeschreibung vorgelegen, welche auch die technischen und organisatorischen Maßnahmen umfassen.
- AixConcept überzeugt sich (vor Ort oder nach Aktenlage) von den technischen und organisatorischen Maßnahmen.
- AixConcept dokumentiert die Kontrollen bei dem Auftragnehmer.