Vertrag zur Auftragsverarbeitung gemäß Artikel 28 Datenschutz-Grundverordnung (DSGVO)[1]

Die

AUGIAS-Data GmbH
Im Südfeld 20
48308 Senden

– Auftragsverarbeiter [2] –

verpflichtet sich gegenüber

<Institution/Firma/Auftraggeber>
vertreten durch: <Person>
<Adresse>
<PLZ Ort>

– Verantwortlicher –

nach Maßgabe der folgenden Bestimmungen:

1. Allgemeines

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen 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 sowie Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtline 95/46/EG (Datenschutz-Grundverordnung).

2 Es gelten die Begriffsbestimmungen der Datenschutz-Grundverordnung.

3. Rechte und Pflichten des Verantwortlichen

(1) Der Auftraggeber ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragsverarbeiter. Dem Auftragsverarbeiter 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 Auftragsverarbeiter wird den Verantwortlichen unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragsverarbeiter geltend machen.

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

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

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

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Verantwortlichen erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragsverarbeiter ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragsverarbeiter 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 Auftragsverarbeiter untersagt, es sei denn, dass der Verantwortliche dieser schriftlich zugestimmt hat.

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

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

(4) Der Auftragsverarbeiter 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 Auftragsverarbeiter wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Verantwortlichen abstimmen.

(5) Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darüber informieren, wenn eine vom Verantwortlichen erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Sofern der Auftragsverarbeiter darlegen kann, dass eine Verarbeitung nach Weisung des Verantwortlichen zu einer Haftung des Auftragsverarbeiters nach Art. 82 DSGVO führen kann, steht dem Auftragsverarbeiter 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 Verantwortlichen außerhalb von Betriebsstätten des Auftragsverarbeiters oder Subunternehmern ist nur mit Zustimmung des Verantwortlichen in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Verantwortlichen in Privatwohnungen ist nur mit Zustimmung des Verantwortlichen in Schriftform oder Textform im Einzelfall zulässig.

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

5. Datenschutzbeauftragter des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat.

(2) Schriftliche Bestellung gemäß Art. 38 und 39 DSGVO – der Auftragsverarbeiter hat als Datenschutzbeauftragten schriftlich bestellt:

Datenschutzbeauftragter: **René Rautenberg**,
ER-Secure René Rautenberg GmbH, In der Knackenau 4, 82031 Grünwald bei München

Datenschutzkooordinator und Ansprechpartner: **Dr. Robert Hartung**,
AUGIAS-Data GmbH, Im Südfeld 20, 48308 Senden

6. Meldepflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter 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 Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet.

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

(3) Dem Auftragsverarbeiter 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 Auftragsverarbeiter wird den Verantwortlichen bei der Umsetzung der Meldepflichten unterstützen. Der Auftragsverarbeiter 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 Auftragsverarbeiters 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 Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach den Artt. 12 – 23 DSGVO. Es gelten die Regelungen der Ziffer 11 dieses Vertrages.

(2) Der Auftragsverarbeiter 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 Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artt. 32 – 36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse des Verantwortlichen

(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 Auftragsverarbeiter jederzeit im erforderlichen Umfang zu kontrollieren.

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

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

(4) Der Verantwortliche kann, im Regelfall nach vorheriger Anmeldung mit angemessener Frist, die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragsverarbeiters zu den jeweils üblichen Geschäftszeiten vornehmen. Er wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragsverarbeiters durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragsverarbeiter 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 zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Verantwortliche ist über entsprechende geplante Maßnahmen vom Auftragsverarbeiter zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unter-Auftragsverarbeitern durch den Auftragsverarbeiter ist nur mit Zustimmung des Verantwortlichen in Textform zulässig.

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

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

(4) Der Auftragsverarbeiter hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Verantwortlichen auch gegenüber dem Unter-Auftragsverarbeiter gelten.

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

(6) Der Auftragsverarbeiter ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Verantwortlichen und von Aufsichtsbehörden auch gegenüber dem Unter-Auftragsverarbeiter gelten und entsprechende Kontrollrechte von dem Verantwortlichen und den Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unter-Auftragsverarbeiter 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 Auftragsverarbeiter 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 Auftragsverarbeiter für den Verantwortlichen erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragsverarbeiter 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-Systemen 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 Auftragsverarbeiter 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 Auftragsverarbeiter verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Verantwortlichen obliegen. Der Verantwortliche ist verpflichtet, dem Auftragsverarbeiter etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragsverarbeiter sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit deren Anwendung vertraut ist. Der Auftragsverarbeiter sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragsverarbeiter 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 ist dem Verantwortlichen auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

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

(2) Soweit eine Mitwirkung des Auftragsverarbeiters für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Verantwortlichen erforderlich ist, wird der Auftragsverarbeiter die jeweils erforderlichen Maßnahmen nach Weisung des Verantwortlichen treffen. Der Auftragsverarbeiter wird den Verantwortlichen 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 Verantwortlichen beim Auftragsverarbeiter 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

Vergütungen des Auftragsverarbeiters werden gesondert vereinbart und sind nicht Gegenstand dieses Vertrages.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragsverarbeiter 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 2** 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 Auftragsverarbeiter 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 Auftragsverarbeiter ohne Abstimmung mit dem Verantwortlichen umgesetzt werden. Der Verantwortliche kann jederzeit eine aktuelle Fassung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragsverarbeiter 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 Auftragsverarbeiter den Verantwortlichen informieren.

15. Dauer des Auftrags

(1) Der Auftragsverarbeiter führt für den Verantwortlichen Leistungen durch. Zwischen den Parteien besteht diesbezüglich ein Vertragsverhältnis (»Hauptvertrag«), das entweder auf individuellen vertraglichen Vereinbarungen, allgemeinen Geschäftsbedingungen oder auf gesetzlichen Regelungen (z. B. BGB) basiert. Dieser Vertrag beginnt ab der Unterzeichnung durch beide Parteien und gilt für die Dauer des jeweiligen Hauptvertrages.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragsverarbeiter 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. Et-

waige 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 Auftragsverarbeiter zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragsverarbeiters erfolgen.

(3) Der Auftragsverarbeiter darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragsverarbeiter 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. Schlussbestimmungen

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

_____	_____	_____	_____
Ort	Datum	Ort	Datum
_____		_____	
Verantwortlicher (Druckschrift)		Auftragsverarbeiter (Druckschrift)	
_____		_____	
Verantwortlicher (Unterschrift)		Auftragsverarbeiter (Unterschrift)	

Anlage 1
Gegenstand des Auftrags

1. Datenschutzbeauftragter des Verantwortlichen

(oder Ansprechpartner, falls kein Datenschutzbeauftragter bestellt ist):

<Name>
<Adresse>
<PLZ Ort>
<Tel.>, <E-Mail>

2. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Verantwortlichen an den Auftragsverarbeiter umfasst folgende Arbeiten und/oder Leistungen:

- Remote-Service bzw. Fernwartung
- Datenübertragung zur Problembeseitigung
- Fehleranalyse und Fehlerklärung mit Nutzerdaten
- Datenmigration und Konvertierung von Daten
- Sonstige Dienstleistungen

3. Art der personenbezogenen Daten

Folgende Datenarten sind Gegenstand der Verarbeitung:

- Benutzer-/Anwenderdaten, Adressen, Geburtsdaten, Telefonnummern, E-Mail
- name, Adresse, Kontaktdaten von Personen, die Archivgut aus Nachlässen, Sammlungen oder Schenkungen überlassen haben,
- Archivgut mit personenbezogenen Daten wie bspw. Verwaltungsakten

4. Kategorien betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:

- Mitarbeiter
- Nutzer, Überlasser von Archivgut, im Archivgut gespeicherte Personen

Anlage 2
Technisch-organisatorische Maßnahmen

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die AUGIAS-Data GmbH erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1 Zutrittskontrolle

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Manuelles Schließsystem	☒ Empfang / Rezeption / Pförtner
☒ Schließsystem mit Codesperre	☒ Besucher werden von Mitarbeitern begleitet
☒ Türen mit Knauf Außenseite	☒ Sorgfalt bei Auswahl Reinigungsdienste

1.2 Zugangskontrolle

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Login mit Benutzername + Passwort	☒ Zentrale Passwortvergabe
☒ Anti-Viren-Software Server	☒ Richtlinie »Sicheres Passwort«
☒ Anti-Virus-Software Clients	☒ Richtlinie »Löschkonzept«
☒ Anti-Virus-Software mobile Geräte	☒ Allg. Datenschutz-Richtlinie
☒ Firewall	
☒ Intrusion Detection Systeme	
☒ Verschlüsselung von Datenträgern	

1.3 Zugriffskontrolle

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Aktenshredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Physische Löschung von Datenträgern	☒ Minimale Anzahl an Administratoren
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei Eingabe, Änderung und Löschung von Daten	☒ Verwaltung der Benutzerrechte durch Administratoren

1.4 Trennungskontrolle

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	

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

2.1 Weitergabekontrolle

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Email-Verschlüsselung	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Protokollierung der Zugriffe und Abrufe	
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	

2.2 Eingabekontrolle

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Technische Maßnahmen	*Organisatorische Maßnahmen*
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☒ Klare Zuständigkeiten für Löschungen

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

3.1 Verfügbarkeitskontrolle

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☒ Serverraumüberwachung Temperatur	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ USV (unterbrechungsfreie Stromversorgung)	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ Schutzsteckdosenleisten Serverraum	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ RAID System / Festplattenspiegelung	

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

4.1 Datenschutz-Management

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz, mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf und Berechtigung	☒ Externer Datenschutzbeauftragter: ER-Secure.de

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Anderweitiges dokumentiertes Sicherheitskonzept: QM-System nach DIN EN ISO 9001:2015	☒ Mitarbeiter geschult und auf Vertraulichkeit und das Datengeheimnis verpflichtet
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
	☒ Interner IT-Sicherheitsbeauftragter: IT-Abteilung
	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident-Response-Management

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Einsatz von Firewalls und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf die Meldepflicht gegenüber den Aufsichtsbehörden)
☒ Einsatz von Spamfiltern und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscannern und regelmäßige Aktualisierung	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☒ Intrusion Detection System (IDS)	
☒ Intrusion Prevention System (IPS)	

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

Technische Maßnahmen	*Organisatorische Maßnahmen*
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Technische Maßnahmen	*Organisatorische Maßnahmen*
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)

Weitere Maßnahme:

Fremddaten (z. B. zur Konvertierung) werden grundsätzlich nur durch interne Mitarbeiter bearbeitet.