Vertrag zur Auftragsverarbeitung

zwischen

- Auftraggeber -

und

BSS Business Solutions for Services – OST GmbH

Köpenicker Str. 325
12555 Berlin

- Auftragnehmer -

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Vertrag i.S.d. Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

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

Vertragsgegenstand ist die Fernbetreuung der im Projektrahmenauftrag und dessen Anlagen beschriebenen und gemäß den dortigen Bestimmungen lizenzierten Softwaremodelle sowie die Lieferung der von Microsoft bzw. der Haveldata GmbH während der Vertragslaufzeit allgemein zum Vertrieb in Deutschland freigegebenen Update Versionen. Als Plattform kann auch ein Cloudmodell von Microsoft in Anwendung kommen. Hier handelt es sich um die Europa oder Deutschland Cloud von Microsoft. Update-Versionen dienen der Pflege der aktuellen Version der im Projektrahmenvertrag beschriebenen Software. Voraussetzung hierfür ist ein gültiger Enhancement Plan für die Software. BSS übernimmt die Betreuung sämtlicher in dem im Projektrahmenauftrag und dessen Anlagen genannten Programmteile sowie die Erweiterungen und Anpassungen. Die Wartung von Computerhardware gehört nicht zum Vertrag, ebenso wenig die Lieferung neuer Module und Add-Ons der Software. Die vertraglichen Pflegedienste der BSS erstrecken sich auf Fehlerbeseitigung des Programmcodes, die Einarbeitung von Veränderungen rechtlicher Anforderungen, die Verbesserung bestehender Programmfunktionalitäten bzw. die Erweiterung bestehender Module mit zusätzlichen Modulen, die Beratung des Kunden laut aktuellen Servicebedingungen bei Fragen und Problemen hinsichtlich der Benutzung der

Software, soweit dort die Onlinehilfe bzw. die Schulungsunterlagen im Einzelfall nicht ausreichen sowie bei ggf. zu verzeichnenden Programmfehler und die Erläuterung der Funktionen und die Handhabung der Lizenzprogramme laut aktueller Servicebedingungen, sowie den von BSS vorgenommenen Anpassungen, soweit dort die Onlinehilfe bzw. die Schulungsunterlagen im Einzelfall nicht ausreichen. Folgende Punkte gehören ebenso zu den Aufgaben, wie Beratung und Betreuung des Kunden in Softwarefragen, Hilfestellung in Fernwartungen und Informationen über aktuelle Entwicklung der Standartapplikationen, Beratung zu Problemlösung aller Hardware- und softwaretechnischen Probleme des Datenbankservers.

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Eine regelmäßige Verarbeitung von personenbezogenen Daten erfolgt nicht. Bei der unter Punkt 2 beschriebenen Fernbetreuung ist jedoch nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf folgende Daten/Datenarten hat:

- Adressdaten (Kunden, Lieferanten, und Mitarbeiter)
- Sozialversicherungsdaten
- Nutzungsdaten (Protokolle)

Kreis der von der Datenverarbeitung Betroffenen:

- Kunden
- Lieferanten
- Mitarbeiter

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 6 das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässige Datenverarbeitungen hinzuweisen. 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.

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

(3) Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren.

(4) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können

☒ schriftlich
☒ per Fax
☒ per E-Mail
☐ mündlich

erfolgen. Der Auftraggeber soll mündliche Weisungen, sofern diese in diesem Vertrag für Weisungen zulässig sind, unverzüglich in Textform (z.B. Fax, E-Mail,) gegenüber dem Auftragnehmer bestätigen.

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

(6) Der Auftraggeber kann weisungsberechtigte Personen benennen. Weisungsberechtigte Personen des Auftraggebers sind:

Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.

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

(8) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach § 15a TMG, Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragsverarbeiter 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. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(2) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

(3) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Die Pflicht zur Bestätigung kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen

Datenschutzbeauftragten zu bestellen 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.

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

(5) 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.

(6) 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.

(7) 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. 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.

(8) Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

- besondere Arten personenbezogener Daten (Art. 9 DSGVO) oder
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder (auch i.S.v. Art. 10 DSGVO)
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

(9) 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 nicht zulässig.

(10) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragnehmer die Daten mit dem jeweiligen Zweck kennzeichnen.

(11) An der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen. Der Auftragnehmer legt dem Auftraggeber, auf Verlangen, die den Auftrag betreffenden Verzeichnisse von Verarbeitungstätigkeiten vor.

(12) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-35 DSGVO genannten Pflichten.

(13) Der Auftragnehmer soll dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

Weisungsempfangsberechtigte Personen des Auftragnehmers sind:

Yves-Stefan Pade
Stephan Weikelt
Bernd Kutz

5. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

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

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

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

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber 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.

6. Unterauftragsverhältnisse

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

7. Datengeheimnis / Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer wird alle Beschäftigten, die Leistungen im Zusammenhang mit dem Auftrag des Auftraggebers erbringen, in schriftlicher Form verpflichten, alle Daten des Auftraggebers, insbesondere die für den Auftraggeber verarbeiteten personenbezogenen Daten vertraulich zu behandeln. Diese Verpflichtung der Beschäftigten ist auf Anfrage dem Auftraggeber nachzuweisen.
Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis i.S.d. § 88 TKG zu verpflichten.

8. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

9. 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.

10. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

11. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

(2) 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 Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

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

(4) Auftragnehmer wird dem Auftraggeber die von ihm nach Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung des nach Art. 32 DSGVO und des in diesem Vertrag geregelten Schutzniveaus in dokumentierter Form und in geeigneter Weise zur Verfügung stellen. Sofern die Parteien nicht gesondert vereinbaren, dass die in der „**Anlage 2“** aufgeführten technischen und organisatorischen Maßnahmen durch die nach diesem Absatz neu zur Verfügung gestellte Dokumentation der technischen und organisatorischen Maßnahmen zur Datensicherheit ersetzt werden, bleiben die in „Anlage 2“ genannten Maßnahmen Vertragsbestandteil und sind vom Auftragnehmer entsprechend zu erfüllen.

12. Dauer des Auftrags

(1) Der Vertrag beginnt am _____ und wird auf unbestimmte Zeit geschlossen.

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

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

13. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

(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.

14. Zurückbehaltungsrecht

(1) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

15. Schlussbestimmungen

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

(2) Für Nebenabreden ist die Schriftform erforderlich.

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

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

Anlage 1
Unterauftragnehmer

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

Dabei handelt es sich um nachfolgende(s) Unternehmen:

haveldata GmbH
Bahnhofspassage 4
14776 Brandenburg an der Havel

gbedv GmbH & Co. KG
Loger Str. 22 b
27711 Osterholz-Scharmbeck

BSS Business Solutions for Services GmbH
Koenigstor 35
34117 Kassel

Microsoft Corporation
One Microsft Way
Redmond, WA 98052-6399
USA

Microsoft Ireland Operations, Ltd.
Attn: Data Protection
One Microsoft Place,
South County Industrial Park,
Leopardstown,
Dublin 18,
D18 P521

TERRA CLOUD GmbH
Hankamp 2
32609 Hüllhorst

Anlage 2
Gemäß Art. 32 DS-GVO zu Technische und organisatorische Maßnahmen des Auftragnehmers

1. Zutrittskontrolle

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

Die Räume der BSS Business Solutions for Services Ost GmbH (i. F. BSS) befinden sich im Innovationspark Wuhlheide.

Der Zutrittsschutz erfolgt durch folgende Maßnahmen:

- Absicherung von Gebäudeschächten
- Schließsystem
- Manuelles Schließsystem
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal

2. Zugangskontrolle

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

Der Zugang zu den Systemen wird durch ein Rollenkonzept geregelt. In diesem Rollenkonzept sind die Benutzerrechte der jeweiligen Benutzerprofile (Windows-Domäne) dokumentiert.

Den jeweiligen Benutzer wird durch den Administrator eine Rolle zugewiesen. Die personalisierte Authentifikation an den Systemen erfolgt über Benutzername / Passwort.
Die Passwörter (gem. BSI Passwortrichtlinie) werden durch die Benutzer vergeben und regelmäßig geändert.

Die Server befinden sich im Rechenzentrum der Microsoft Europa-Cloud und der TERRA CLOUD GmbH Deutschland.

Für die Verbindung zu Kundensystemen wird nach Absprache mit dem Kunden VPN-Technologie genutzt.

Für Außentermine wird eine verschlüsselte (SHA-256) mobile Festplatte genutzt. Sensible Daten auf Notebooks werden durch sog. TrueCrypt-Container (verschlüsselte Ordner) gesichert.

Zum Virenschutz wird die Antivieren Software der Firma Kaspersky (automatisierte tägl. Updates) und die Windows-Software Defender genutzt.

Zum Schutz vor unerwünschten Netzwerkzugriffen werden am Standort Berlin eine Zyxel Firewall (Hardware) und die Windows-Firewall (Software) eingesetzt.

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Zugriffsrechte verwaltet (Vergabe/Entzug) ein Systemadministrator. Sie sind im Berechtigungskonzept geregelt. Die Anzahl der Systemadministratoren ist auf das „Notwendigste“ reduziert.

Der Zugriff auf die Daten erfolgt über personalisierte Anmeldungen. Die Passwörter entsprechen der BSI-Passwortrichtlinie (sieh Punkt 2). Die Zugriffe, insbesondere bei der Eingabe, Änderung und Löschung von Daten, werden protokolliert.

Datenträger werden in verschlossenen Räumen (bzw. Schränken) aufbewahrt. Zur physischen Löschung von Datenträgern vor Wiederverwendung wird die Software CCleaner genutzt.
Zur Außerbetriebnahme von Datenträgern werden diese im Haus durch eigenes Personal vernichtet. Die Vernichtung wird protokolliert.

Papierdokumente werden mit Aktenvernichtern durch eigenes Personalvernichtet.

4. Weitergabekontrolle

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

Um unbefugte Benutzung von Daten zu verhindern, wird bei der Verbindung zu Kundensystemen ein VPN-Tunnel aufgebaut.

Die Weitergabe von Daten erfolgt gemäß Absprache mit dem Kunden in anonymisierter oder pseudonymisierter Form (Verfahren wird abgesprochen). Eine Weitergabe an unberechtigte Dritte erfolgt nicht.

Die Daten werden nur gemäß den vereinbarten Regelungen (z.B. AV) vorgehalten und gelöscht.

Sollten Daten physisch (z.B. mobile Festplatte – Vor-Ort Termin) transportiert werden, dann erfolgt dieser Transport nur durch eigens Personal in sicheren Transportbehältnissen.

5. Eingabekontrolle

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

Eingaben (z.B. Ändern und Löschen von Daten) werden protokolliert. Durch die personalisierte Anmeldung an den Systemen kann in den Protokollen nachvollzogen werden, wer (Benutzername) bestimmte Eingaben durchgeführt hat.

Die Vergabe von Berechtigungen zur Eingabe, Änderung und Löschung von Daten geschieht auf Basis des Berechtigungskonzepts.

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die Rechte und Pflichten von Auftraggeber und Auftragnehmer sind in einem Auftragsverarbeitungsvertrag gem. DS-GVO geregelt. Durch diesen Vertrag wird u.a. sichergestellt, dass folgende Punkte berücksichtigt werden:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (Artikel 5 DS-GVO)
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7. Verfügbarkeitskontrolle

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

Daten werden in der Microsoft Europa-Cloud und in der Terra Cloud von der TERRA CLOUD GmbH gespeichert.
Die Microsoft Europa-Cloud wird in zertifizierten Rechenzentren betrieben, die die Verfügbarkeit der Daten gewährleisten.
Zum Schutz gegen Zerstörung und Verlust der Daten wurden folgende Maßnahmen am Standort Berlin umgesetzt:

- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung

8. Trennungsgebot

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

Typische Maßnahmen (nur Stichworte) sind z.B.:

- Logische Mandantentrennung (softwareseitig)
- Physikalische Trennung von Produktiv- und Testsystem