Auftragsverarbeitungsvertrag (AVV)

zwischen

Kunde
Kundenadresse

-als Verantwortlicher (hier bezeichnet als „Auftraggeber“) -

und

Ehler Philipp GmbH
Haus für Büroausstattung
Große Straße 65

27283 Verden

-als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“) -

Präambel

Auftraggeber und Auftragnehmer sehen sich den hohen Standards verpflichtet, die durch die Datenschutzgrundverordnung und andere datenschutzrechtlichen Vorschriften gelten. Zur Sicherung der Vertraulichkeit und Wahrung aller einschlägigen datenschutzrechtlicher Bestimmungen schließen die Parteien nachfolgende Vereinbarungen, die Anwendung auf alle Tätigkeiten finden, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Der vorliegende Auftragsverarbeitungsvertrag (kurz: „AVV“) konkretisiert für alle Verarbeitungen die Rechte und Pflichten der Parteien auf dem Gebiet des Datenschutzes, welche sich aus den zwischen den Parteien bereits oder künftig bestehenden rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnissen (kurz: „Hauptvertrag“) ergeben.

Der AVV kommt mit all seinen Teilen zur Anwendung, sofern der Auftraggeber den Auftragnehmer zur Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO (kurz: „Daten“) verpflichtet hat. Der AVV bildet den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten« im Sinne des Art. 4 Nr. 1 DSGVO) des Auftraggebers verarbeiten.

Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV und all seiner Teile den Regelungen des zugehörigen Hauptvertrages vor.

Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (kurz: „Spezifika“) werden vor Beginn der Verarbeitung geregelt. Dies sind insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorie der Daten und die Kategorien betroffener Personen, die Übersicht über Subauftragsnehmer sowie die technischen und organisatorischen Maßnahmen (kurz: „TOMs“).

1. Gegenstand und Dauer des Auftrags

(1) Zwischen den Parteien besteht ein Vertragsverhältnis („Hauptvertrag“) über die Einrichtung, Wartung und Pflege von IT-Systemen. IT-Systeme meinen in diesem Kontext auch explizit Druck- und Multifunktionssysteme sowie Scanner und anhängige Software. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Einrichtung, Wartung und Pflege von IT-Systemen durchzuführen oder durchführen zu können.

(2) Diese Vereinbarung zur Auftragsverarbeitung beginnt ab Unterzeichnung durch beide Parteien und gilt für die Dauer des jeweiligen Hauptvertrages.

(3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen der DSGVO oder dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert.

(4) Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

2. Art und Zweck der Datenverarbeitung

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

- Installation und Wartung von Druck- und Multifunktionssystemen
- Installation und Wartung von Softwarelösungen
- Monitoring von IT- und Drucksystemen
- Beratungsdienstleistungen
- Fernwartung zur Problemanalyse und –Behebung
- Durchführung von Einweisungen, Schulungen vor Ort oder per Web / Telefon

Hierbei ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf folgende Daten/ Datenarten hat:

- Unternehmenskorrespondenz mit z.B. Lieferanten, Kunden, Partnern
- Buchhaltungsdaten
- Login-Daten
- Nutzungs- und Bestandsdaten
- Personaldaten

Kreis der von der Datenverarbeitung Betroffenen:

- Kunden und deren Ansprechpartner
- Interessenten
- Beschäftigte
- Lieferanten, Handelsvertreter, Partner

3. Zusammenarbeit und Ansprechpartner

(1) Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Der Auftragnehmer handelt ausschließlich weisungsgebunden, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten, die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

(4) Macht eine betroffene Personen Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(5) Soweit der Auftraggeber einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

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

(7) Die Parteien benennen gegenseitig einen oder mehrere Ansprechpartner in datenschutzrechtlichen Angelegenheiten.

Ansprechpartner in datenschutzrechtlichen Angelegenheiten des Auftraggebers ist/sind:

_____

_____

Bestellter Datenschutzbeauftragter beim Auftraggeber ist:

Name _____

Tel.: _____

E-Mail: _____

Ansprechpartner in datenschutzrechtlichen Angelegenheiten bei der Ehler Philipp GmbH ist: **Herr Marc Philipp**

Bestellter Datenschutzbeauftragter bei der Ehler Philipp GmbH ist:
Herr Dr. Uwe Nolte, Tel.: +49 160/6322232, E-Mail: info@datenschutz-qm.de

Ergeben sich bei den Ansprechpartnern und Datenschutzbeauftragten Änderungen, haben sich die Parteien hierüber in Textform zu informieren.

4. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Wartung und Pflege von IT-Systemen gegenüber dem Auftragnehmer zu erteilen. Weisungen können schriftlich, per Fax, per E-Mail oder mündlich erfolgen.

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

(3) 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. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle erforderlich ist.

(4) Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Auftragnehmer zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.

(5) Der Auftragnehmer darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen die Beauftragung dieses Prüfers ein Einspruchsrecht.

(6) Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien umzusetzende Maßnahmen ab.

(7) Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Auftragnehmer unverzüglich hierüber zu informieren und das weitere Vorgehen mit ihm abzustimmen. Mündliche Unterrichtungen sind unverzüglich in Textform nachzureichen.

5. Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, auf die er im Zusammenhang mit den Wartungs-/Pflegearbeiten Zugriff erhält, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(2) Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der Daten befugten Personen die Weisungen des Auftraggebers kennen und diese beachten.

(3) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(4) Der Auftragnehmer weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Für die Überprüfung der Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüften Wirksamkeit kann der Auftragnehmer auf geeignete Prüfungsnachweise oder auf angemessene Zertifizierungen verweisen.

(5) Angemessen sind zur Darlegung der Umsetzung solcher Maßnahmen aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder geeignete Zertifizierungen durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz), die ergänzend vorgelegt werden. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen oder den Datenschutz verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf der Auftragnehmer jederzeit ablehnen.

(7) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes von Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Auftragnehmer besteht. Mündliche Unterrichtungen sind in Textform nachzureichen. Der Auftragnehmer stimmt sich zur Behandlung solcher Verletzungen mit dem Auftraggeber ab. Die Parteien treffen die erforderlichen Maßnahmen, einschließlich der Maßnahmen zur Minderung möglicher nachteiliger Folgen.

(8) Der Auftraggeber ist über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, sofort zu informieren. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (kurz: „Sperrung“), wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

(10) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber in Textform zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich in Textform darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.

6. Fernwartung

(1) Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die es dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

(2) Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

(3) Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

7. Unterauftragsverhältnisse

(1) Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (kurz: „Unterauftragnehmer“) erbringen lassen. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

(2) Der Auftragnehmer informiert den Auftraggeber rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt.

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

(4) Die Verpflichtung des Unterauftragnehmer muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

(5) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(6) Eine Beauftragung von Unterauftragnehmer in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln) erfüllt sind. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmer deutlich voneinander abgegrenzt werden

(7) Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt Dazu zählen z.B. Post, Telekommunikationsleistungen, reine technische Wartung, Reinigungskräfte, Prüfer.

(8) Für die Durchführung der vereinbarten Auftragsverarbeitung durch den Auftragnehmer werden keine Unterauftragsnehmer im Sinne des Art. 28 (4) eingesetzt.

8. Übermittlung von Daten an einen Empfänger in einem Drittland

(1) Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln) erfüllt sind. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmer deutlich voneinander abgegrenzt werden.

9. Wahrung von Betroffenenrechten

Der Auftraggeber ist für die Wahrung der Betroffenenrechte alleinig verantwortlich. Der Auftragnehmer hat den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nachzukommen.

10. Sicherheit der Verarbeitung

(1) Die Parteien vereinbaren technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten. Die TOMs des Auftragnehmers sind in der Anlage aufgeführt.

(2) Änderung der vereinbarten TOMs bleiben dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen.

(3) Trifft der Auftraggeber eigene technische und organisatorische Maßnahmen für eine auf den Auftragnehmer übertragene Datenverarbeitung, so hat ihn der Auftragnehmer im Rahmen seiner Möglichkeiten hierbei zu unterstützen. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

11. Beendigung und Löschung von Daten

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach dessen Wunsch datenschutzkonform zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren.

(2) Gleichgültig, aus welchem Grund das Vertragsverhältnis zwischen den Parteien endet, steht dem Auftragnehmer kein Zurückbehaltungsrecht an den Daten oder Unterlagen zu.

(3) 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.

(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Haftung und Schadenersatz

(1) Macht ein Betroffener gegenüber einer Partei Schadenersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

(2) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(3) Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei oder zur Aufsichtsbehörde gefährden.

13. Schlussbestimmungen

(1) Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

(2) Sollten einzelne Teile dieser Vereinbarung ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen gleichwohl aufrechterhalten und gültig. Anstelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch insoweit verpflichtet, unverzüglich eine rechtswirksame und datenschutzkonforme Vertragsergänzung abzustimmen und zu erstellen

(3) Es gilt das Recht der Bundesrepublik Deutschland.

Ort, Datum	Ort, Datum
- Unterschrift Auftraggeber -	- Unterschrift Auftragnehmer -

Anlage – Technisch-organisatorische Maßnahmen (TOMs)

1. Vertraulichkeit

(Art. 32 Abs. 1 b DSGVO)

Zutrittskontrolle

Kein unbefugter Zutritt zu Gebäuden und Datenverarbeitungsanlagen, z.B.: Sicherheitsschlösser, Chipkarten, Sicherheitsverglasung, Alarmanlagen, Videoanlagen

☑ Schlüssel/Transponderregelung
☑ Sicherheitsschlösser
☑ Sicherheitstüren / -fenster
☑ Klingelanlage mit Kamera
☑ Sorgfältige Auswahl der Reinigungsdienste
☑ Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz
☑ gesicherter Zutritt zum Rechenzentrum
☑ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups / Datenträgern

Zugangskontrolle

Keine unbefugte Systembenutzung, z.B. Serverschrank verschlossen, Benutzerkennung mit Passwort, Firewall, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern

☑ Verschluss von Datenverarbeitungsanlagen
☑ Zuordnung von Benutzerrechten
☑ Login mit Benutzername + Passwort
☑ Automatische Sperrung von Nutzer-Accounts nach mehrfacher Fehleingabe von Passwörtern
☑ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
☑ Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität
☑ Zwei-Faktor-Authentifizierung
☑ Mobile Device Management-System
☑ Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
☑ Prozess zum Rechteentzug bei Austritt von Mitarbeitern
☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis
☑ Verschlüsselung von Smartphone-Inhalten
☑ Anti-Viren-Software
☑ Automatische Sperrmechanismen bei Mobil-Geräten
☑ Firewall

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B. Berechtigungskonzept, bedarfsgerechte Zugriffsrechte, Benutzerkennung mit Passwort, gesicherte Schnittstellen (USB, Netzwerk, etc.), Protokollierung von Zugriffen

☑ Berechtigungskonzept, Profile/Rollen

☑ Anzahl der Administratoren auf das „Notwendigste“ reduziert

☑ Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)

☑ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☑ Konzept der Laufwerksnutzung und -Zuordnung

☑ Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)

☑ Netzsegmentierung

☑ Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken

☑ Protokollieren von Dateizugriffen

☑ Zeitliche Begrenzung der Zugriffsmöglichkeiten

☑ Anti-Viren-Software

☑ Schadsoftware-Filterung für Web

☑ Schadsoftware-/Spam-Filterung für E-Mail

☑ Firewall

☑ Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von pb Daten Gegenstand der Dienstleistung ist.

☑ Mobile Device Management-System

☑ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)

☑ Aktenschredder (mind. Stufe 3, cross cut)

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Trennung von Produktiv- und Testsystemen, Mandantenfähigkeit, getrennte Ordnerstrukturen, getrennte Datenbanken, Virtualisierung

☑ Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)

☑ Datentrennung durch Netzsegmentierung

☑ Berechtigungskonzept

☑ Laufwerkstrennung, verschiedene logische Laufwerke

☑ Trennung von Entwicklungs-, Test- und Produktivsystem

☑ Virtualisierung

2. Pseudonymisierung

(Art. 32 Abs. 1 a DSGVO; Art. 25 Abs. 1 DSGVO)

Durch die Verschleierung von Daten sowie die Entfernung von Bezügen (Pseudonymisierung) wird gewährleisten, dass eine Zuordnung der Daten zu einer spezifischen betroffenen Person ohne Kenntnis oder Hinzuziehung zusätzlicher Informationen nicht mehr möglich ist.

☑ es findet keine Pseudonymisierung statt

3. Integrität

(Art. 32 Abs. 1 b DSGVO)

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B. Verschlüsselung, VPN, Firewall, elektronisch Signatur, Fax-Protokoll

☑ Getunnelte Datenfernverbindungen (VPN)

☑ Berechtigungskonzept

☑ Protokollierung von Datenübertragung oder Datentransport

☑ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten

☑ Fernwartungskonzept (Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort etc.)

☑ Mobile Device Management-System

☑ Gesicherter Eingang für Anlieferung und Abholung

☑ Aufbewahrung personenbezogener Daten in verschließbaren Sicherheitsschränken

☑ Kontrollierte Vernichtung von Papier/Datenträger

☑ Schredder Sicherheitsstufe gem. DIN 66399

☑ Dokumentation der Übermittlungsstellen und -wege

☑ Verpackungs- und Versand Vorschriften

☑ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen

☑ Firewall

Eingabekontrolle

Festlegung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt werden dürfen, z.B. Protokollierung. Benutzeridentifikation, Dokumentenmanagement

☑ Berechtigungskonzept, Rollen/Profile

☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☑ Systemseitige Protokollierung von Dateneingaben / -löschungen

☑ Verpflichtung auf das Datengeheimnis

☑ Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke

☑ Dokumentenmanagementsystem

Verschlüsselung

☑ Verschlüsselung von Smartphones und Tablets

☑ Verschlüsselung von Laptops

☑ Verschlüsselte Aufbewahrung von Passwörtern

☑ Verschlüsselter E-Mail-Versand (Transportverschlüsselung)

☑ Verschlüsselung von Online-Diensten (HTTPS)

☑ Verschlüsselung bei Speicherung in Clouds und anderen externen Storage-Lösungen

☑ Verschlüsselung bei Übertragung über Funk-Netzwerke (WLAN)

4. Verfügbarkeit und Belastbarkeit

(Art. 32 Abs. 1 b DSGVO)

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B. Brandschutz, Überspannungsschutz, USV, Klimaanlage, RAID, Virenschutz, Backup-Strategie

☑ Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal
☑ Brandmeldeanlagen in Serverräumlichkeiten
☑ Wasserlose Brandlöschmittel (z.B. $C0_2$-Löscher) in Serverräumlichkeiten
☑ Klimatisierte Serverräumlichkeiten
☑ Blitz-/Überspannungsschutz
☑ Unterbrechungsfreie Stromversorgung (USV)
☑ RAID-Systeme
☑ Automatische Updates Software und Firmware
☑ Getrennte Partitionen für Betriebssysteme und Daten
☑ Datensicherungs- und Backupkonzept
☑ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
☑ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☑ Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitten
☑ Gewährleistung der technischen Lesbarkeit von Backup-Speichermedien für die Zukunft
☑ Virenschutz
☑ Firewall
☑ Rasche Wiederherstellbarkeit

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Art. 32 Abs. 1 d DSGVO; Art. 25 Abs. 1 DSGVO

Datenschutz-*Management*

Folgende Maßnahmen sollen gewährleisten, dass eine datenschutzrechtliche Organisation vorhanden ist:

☑ Datenschutzleitbild des Unternehmens
☑ Bestellung eines Datenschutzbeauftragten
☑ Meldung neuer/veränderter Prozesse an den Datenschutzbeauftragten
☑ Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO
☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis
☑ Schulungen der Mitarbeiter in Datenschutzangelegenheiten
☑ Führen einer Übersicht über Verarbeitungstätigkeiten
☑ Verzeichnisse von Verarbeitungstätigkeiten werden regelmäßig überprüft und aktualisiert
☑ Datenschutzfreundliche Voreinstellungen, Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
☑ Richtlinien/Anweisungen zur Gewährleistung von technischen und organisatorischen Maßnahmen zur Datensicherheit
☑ Risikoadaptierte technisch-organisatorische Maßnahmen
☑ Jährliche oder anlassbezogene Anpassung der TOMs an Änderungen

☑ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich

☑ Informationssicherheitskonzept

Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Notfällen oder Datenschutz-vorkommen Meldeprozesse ausgelöst werden:

☑ Notfallliste mit sämtlichen Ansprechpartnern

☑ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

☑ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)

☑ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

Auftragskontrolle

eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, z.B. Google, Cloud, Outsourcing IT, Lohn/Gehalt

☑ Vertragsgestaltung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln gemäß gesetzlichen Vorgaben

☑ Sorgfältige Auswahl von Auftragnehmern (insbesondere hinsichtlich Datensicherheit)

☑ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation

☑ Vereinbarung zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers

☑ Schriftliche Weisungen an den Auftragnehmer

☑ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

☑ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer

☑ Regelung zum Einsatz weiterer Subunternehmer

☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis

☑ Sichtung vorhandener IT-Sicherheitszertifikate des Auftragsverarbeiters

☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags