Vereinbarung zur Verarbeitung von Daten im Auftrag

zwischen

_____

_____

_____

_____

– Verantwortlicher –
- nachfolgend Auftraggeber genannt-
-

und

Paul Sonnabend Büro- und Datentechnik GmbH & Co. KG
Steinweg 5
34369 Hofgeismar
– Auftragsverarbeiter –
-nachfolgend Auftragnehmer genannt-

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- ☐ (Fern-) Administration der EDV
- ☐ Wartung von Multifunktionsgeräten
- ☐ Online-Datensicherung
- ☐ Administration der Telefon-Anlage
- ☐ PARTNERasp

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/- kategorien (Aufzählung/ Beschreibung der Datenkategorien):

☒ Abrechnungsdaten	☒ Adressdaten	☒ Bankverbindungsdaten
☐ Biometrische Daten	☒ Bonitätsdaten	☒ Funktionsbezeichnung
☒ Geburtsdatum	☒ Gesundheitsdaten	☒ Interessen
☒ IT-Nutzungsdaten	☐ Kontaktdaten	☒ Lohn- und Gehaltsdaten
☒ Name	☒ Personalstammdaten	☒ Planungsdaten
☒ Qualifikationsdaten	☒ Sozialversicherungsdaten	
☒ Vertragsdaten	☒ Vertragsstammdaten	
☒ Zahlungsdaten	☒ Zeiterfassungsdaten	
☐ Authentifizierungsdaten	☐ Angebotsdaten	
☐ Passwortdateien	☐ Profildaten	
☐ Videoaufzeichnungen	☐ Bilddaten	
☐ E-Mails	☐ Telefonate	

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffener Personen umfassen:

☒ Mitarbeiter	☒ Kunden/ Mandanten	☒ Dienstleister
☒ Bewerber	☒ Interessenten	☐ Handelsvertreter
☒ Auszubildende	☐ Ansprechpartner	☐ Lieferanten
☒ Praktikanten	☐ Veranstaltungsteilnehmer	☐ Berater
☐ Rentner	☐ Abonnenten	
☐ ehemalige Mitarbeiter	☐ Patienten	
☐ Gesellschafter	☒ Besucher	
☐ Mitglieder	☐ Mieter	
☒ Nutzer	☐ Unterhaltsberechtigte	

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(3) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(4) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(5) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(6) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auf-

traggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(7) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch: aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

(8) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 4 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die in der Anlage 1 dargelegten technischen und organisatorischen Maßnahmen umgesetzt. Diese werden Grundlage des Auftrags. Soweit eine Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber auf Anfrage mitzuteilen.

§ 5 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); 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 (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Eine physische Trennung ist nicht zwingend erforderlich.

(3) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 34 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Datenschutzbeauftragte ist derzeit Frau Katharina Bachmann, Datenschutzberatung Moers GmbH, datenschutz@dsb-moers.de. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. 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.

f) Soweit der Auftraggeber seinerseits 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.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 3 dieses Vertrages.

(4) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(5) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO).

§ 7 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

§ 8 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen, wird aber den Verantwortlichen mit ausreichend zeitlichem Vorlauf informieren. Der Auftraggeber darf der Hinzuziehung des Unterauftragsverarbeiters mit Angabe triftiger Gründe widersprechen.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unten der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

C&P Capeletti & Perl Gesellschaft für Datentechnik mbH, Wendenstraße 4, 20097 Hamburg

(3) Ein Wechsel von bestehenden Unterauftragnehmern sind zulässig, soweit:

a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

§ 9 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berück-

sichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

§ 11 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer nicht der EU-DSGVO entsprechenden unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Verantwortlicher und Auftragsverarbeiter im Außenverhältnis gemeinsam als Gesamtschuldner.

(2) Der Auftraggeber trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm selbst verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftraggeber den Auftragnehmer auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragnehmer

erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftraggeber dem Auftragnehmer ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der er den aus der EU-DSGVO resultierenden und speziell den für Auftragnehmer auferlegten Pflichten nicht nachgekommen ist oder er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(4) Für Schäden des Auftraggebers durch schuldhafte Verstöße des Auftragnehmers oder etwaiger Unterauftragsverarbeiter bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

§ 12 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.

§ 13 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.

Anlage 1: Vereinbarung zur Verarbeitung von Daten im Auftrag

Technische und organisatorische Maßnahmen

der

Paul Sonnabend Büro- und Datentechnik GmbH & Co. KG
Steinweg 5
34369 Hofgeismar

Als nicht-öffentliche Stelle, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen wir technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Insbesondere sind Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen. Die folgenden technischen und organisatorischen Maßnahmen[1] sind dazu in unserem Unternehmen umgesetzt:

Die folgenden technischen und organisatorischen Maßnahmen[2] sind dazu in unserem Unternehmen umgesetzt (zutreffendes ist angekreuzt):

1. Vertraulichkeit

a) Zutrittskontrolle/Gebäudeabsicherung

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

☐	Alarmanlage	☐	Absicherung von Gebäudeschächten
☐	Automatisches Zutrittskontrollsystem	☐	Chipkarten-/Transponder-Schließsystem
☐	Schließsystem mit Codesperre	☒	Manuelles Schließsystem
☐	Biometrische Zugangssperren	☐	Videoüberwachung der Zugänge
☐	Lichtschranken / Bewegungsmelder	☒	Sicherheitsschlösser
☒	Schlüsselregelung (Schlüsselausgabe etc.)	☒	Personenkontrolle beim Pförtner / Empfang
☐	Protokollierung der Besucher	☒	Sorgfältige Auswahl von Reinigungspersonal
☐	Einsatz von sorgfältig ausgewähltem Wachpersonal	☒	Einrichtung von abgestuften Sicherheitszonen (Besucherbereich, Büros mit sicherheitsrelevanten Verarbeitungen, Serverräume

[1] Aus den Angaben muss ein angemessenes Sicherheitsniveau ableitbar sein. In jedem Abschnitt sind dazu getroffene Maßnahmen anzugeben.

b) Zugangskontrolle/Absicherung Systemzugang

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

- ☒ Zuordnung von Benutzerrechten
- ☒ Einsatz von individuellen Benutzernamen
- ☒ Vorgaben für sichere Passwörter
- ☐ Authentifikation mit biometrischen Verfahren
- ☒ Authentifikation mit Benutzername/ Passwort
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Gehäuseverriegelungen am Server
- ☒ Einsatz von VPN-Technologie (Fernzugriff)
- ☒ Sperren von externen Schnittstellen (USB etc.)
- ☐ Verschlüsselung von mobilen Datenträgern
- ☒ Einsatz von Intrusion-Detection-Systemen
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum Fern-Löschen)
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☒ Sichere Passwörter für Smartphones
- ☐ Verschlüsselung von Datenträgern in Laptops

c) Zugriffskontrolle/Sicherstellung von Zugriffsberechtigungen

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Ordnungsgemäße Vernichtung von Papier (Einsatz von Aktenvernichtern bzw. Dienstleistern)
- ☐ Physische Löschung von Datenträgern vor Wiederverwendung
- ☒ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☒ Sichere Aufbewahrung von Datenträgern
- ☐ Protokollierung der Vernichtung
- ☐ Verschlüsselung von Datenträgern
- ☒ Einsatz von Anti-Viren-Software
- ☒ Einsatz einer Hardware-Firewall
- ☒ Einsatz einer Software-Firewall

d) Trennungskontrolle/Maßnahmen zur Zwecktrennung von Daten

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing, physikalisch oder virtuell getrennte Systeme.

- ☒ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Logische Mandantentrennung (softwareseitig)
- ☒ Erstellung eines Berechtigungskonzepts
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☒ Trennung von Produktiv- und Testsystem
- ☒ Keine Produktivdaten in Testsystemen

2. Integrität

a) Weitergabekontrolle/Sicherheit beim Datentransfer

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☒ E-Mail-Verschlüsselung
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☒ Verschlüsselung externer Datenträger bei Weitergabe (CDs, USB-Sticks etc.)
- ☐ Verschlüsselte Datenübermittlung (z.B. via https oder SFTP)

b) Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

3. Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle/Schutz von Daten vor zufälliger Zerstörung und Verlust

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Erstellen eines Backup- und Recoverykonzepts
- ☐ Serverräume über der Wassergrenze (nur in Hochwassergebieten relevant)
- ☐ Regelmäßige Sicherung von Systemzuständen
- ☐ Regelmäßige Sicherung von Datenbanken
- ☐ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Erstellen eines Notfallplans
- ☒ Serverräume nicht unter sanitären Anlagen
- ☐ Regelmäßige Sicherung von Dateibeständen

b) Rasche Wiederherstellbarkeit

- ☐ Wiederherstellung nach Backup- und Recoverykonzept
- ☒ Testen von Datenwiederherstellung
- ☐ Kontrolle eines Notfallplans

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Datenschutz-Management

- ☒ Die Grundsätze zum Datenschutz (Erhebung, Verarbeitung oder Nutzung personenbezogener Daten) sind einer unternehmensinternen Richtlinie festgelegt.
- ☒ Es ist ein Datenschutzbeauftragter schriftlich benannt
- ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis / zum Umgang mit personenbezogenen Daten
- ☒ Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis
- ☒ Die interne Verarbeitungsübersicht der Verarbeitungsprozesse ist vorhanden
- ☒ Der DSB ist bei der Datenschutzfolgeabschätzung eingebunden
- ☐ Der DSB ist im Organigramm eingebunden
- ☒ Schulung von Mitarbeitern
- ☐ Einführung eines Kontrollsystems, das den unberechtigten Zugriff auf personenbezogene Daten aufdeckt

b) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

- ☒ Beachtung privacy by Design/Datenschutz durch Technikgestaltung
- ☐ Auswahl datenschutzfreundlicher Technologie bei der Beschaffung
- ☐ Beachtung privacy by Default/Datenschutz durch datenschutzfreundliche Voreinstellungen

c) Auftragskontrolle/Einbindung von Unter-Auftragsverarbeitern

Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

☒ Auswahl der (Unter-)Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

☒ Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z. B. durch Auftragsdatenverarbeitungsvertrag)

☒ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt (wenn erforderlich)

☒ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart

☒ Vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen

☒ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis/ Vertraulichkeit

☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☒ Laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

_____ _____

(Unterschrift des Auftraggebers) **(Unterschrift des Auftragnehmers)**