Vereinbarung über eine Auftragsverarbeitung

zwischen

XXX

(im Folgenden „**Auftraggeber**“)

und

OPTILOHN

(im Folgenden „**Auftragnehmer**“)

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Zusammenhang mit der Auftragsverarbeitung durch den Auftragnehmer bei der Durchführung des zwischen den Parteien geschlossenen Vertrag über die Durchführung der monatlichen Lohnabrechnungen (im Folgenden „**Hauptvertrag**“). Die hierin enthaltenen Vereinbarungen findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Definitionen

(1) Personenbezogene Daten: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person”) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(2) Personenbezogene Daten des Auftraggebers: Personenbezogene Daten des Auftraggebers sind personenbezogene Daten, die der Auftragnehmer für den Auftraggeber erhoben hat oder die der Auftraggeber dem Auftragnehmer bereitgestellt hat.

(3) Datenverarbeitung oder das Verarbeiten von Daten: Datenverarbeitung oder das Verarbeiten von Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(4) Datenverarbeitung im Auftrag: Datenverarbeitung im Auftrag ist Datenverarbeitung durch den Auftragnehmer im Auftrag des Auftraggebers.

(5) Weisung: Eine Weisung erfolgt einerseits durch die Leistungsbeschreibung im Hauptvertrag. Diese ursprüngliche Weisung durch den Hauptvertrag kann durch den Auftraggeber durch zusätzliche schriftliche Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Alle Weisungen sind vom Auftragnehmer zu dokumentieren.

(6) Datenschutzvorschriften: Datenschutzvorschriften meint alle gesetzlichen (Rechts-) Akte der Europäischen Union und/oder ihrer Mitgliedstaaten (insbesondere Gesetze, Richtlinien und Verordnungen) zum Schutz personenbezogener Daten.

(7) EU: EU meint die Mitgliedstaaten der Europäischen Union.

§ 2 Gegenstand und Dauer des Auftrags; Umfang, Art und Zweck der Datenverarbeitung; Art der Daten und Kreis der Betroffenen

(1) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in der Leistungsbeschreibung des Hauptvertrags konkretisiert sind oder zu denen der Auftraggeber dem Auftragnehmer nachträglich eine Weisung erteilt hat.

(2) Die Dauer des Auftrags bestimmt sich nach den Regelungen des Hauptvertrages.

(3) Umfang und Art der Datenverarbeitung bestimmt sich nach der Leistungsbeschreibung des Hauptvertrages in Verbindung mit den Weisungen des Auftraggebers.

(4) Zweck der Datenverarbeitung ist die Erfüllung der in der Leistungsbeschreibung des Hauptvertrages konkretisierten Tätigkeiten durch den Auftragnehmer.

(5) Betroffen von der Verarbeitung sind nachstehende Kategorien von Betroffenen, von denen die gelisteten Arten von Daten verarbeitet werden:

(a) Kategorien der betroffenen Personen:

Beschäftigte der Firma Optilohn

(b) Art der personenbezogenen Daten:

Allgemeine Personendaten, Kennnummern, Bankdaten, physische Merkmale die im Mitarbeiter-Einstellungsbogen aufgelistet werden und für die Erfassung, Verarbeitung und der eigentlichen Lohnabrechnung benötigt werden.

§ 3 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der allgemeinen und technischen und organisatorischen Maßnahmen zu, die erforderlich sind, um ein den jeweils geltenden Datenschutzvorschriften entsprechende(s) Datenschutzniveau bzw. Datensicherheit zu gewährleisten. Insbesondere wird der Auftragnehmer seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen der jeweils geltenden Datenschutzvorschriften gerecht wird. Dies kann insbesondere folgende Maßnahmen beinhalten:

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten des Auftraggebers verarbeitet werden, zu verwehren (**Zutrittskontrolle**),

- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
- dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten des Auftraggebers zugreifen können, und dass personenbezogene Daten des Auftraggebers bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),
- dafür Sorge zu tragen, dass personenbezogene Daten des Auftraggebers 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 des Auftraggebers durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
- dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten des Auftraggebers in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
- dafür Sorge zu tragen, dass personenbezogene Daten des Auftraggebers, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
- dafür Sorge zu tragen, dass personenbezogene Daten des Auftraggebers gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
- dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene, personenbezogene Daten des Auftraggebers getrennt verarbeitet werden können (**Trennungskontrolle**),
- dafür Sorge zu tragen, dass personenbezogene Daten des Auftraggebers pseudonymisiert und verschlüsselt werden können;
- dafür Sorge zu tragen, dass die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt ist;
- dafür Sorge zu tragen, dass die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann;
- dafür Sorge zu tragen, dass ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung eingehalten wird.

(Maßnahmen zur Zugangs-, Zugriffs-, und Weitergabekontrolle sind insbesondere der Einsatz von dem Stand der Technik entsprechender Verschlüsselungsverfahren.)

(2) Der Auftragnehmer hat dem Auftraggeber vor Erteilung des Auftrages ein umfassendes und aktuelles Datenschutz- und Datensicherheitskonzept für diese Auftragsverarbeitung zur Verfügung gestellt, in dem alle technischen und organisatorischen Maßnahmen dargestellt sind. Der Auftragnehmer ist verpflichtet, dieses Datenschutz- und Sicherheitskonzept zu pflegen und fortlaufend zu überprüfen, zu bewerten und zu evaluieren sowie zu aktualisieren, wobei Änderungen mit dem Auftraggeber schriftlich abzustimmen sind. Eine Beschreibung des Datenschutz- und Datensicherheitskonzeptes ist als **Anhang 1** Bestandteil dieser Vereinbarung**.**

(3) Der Auftragnehmer weist dem Auftraggeber die von ihm getroffenen technischen und organisatorischen Maßnahmen auf Anfrage nach; der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch durch Vorlage von Testaten oder Berichten unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- und Datenschutzaudit erbracht werden.

§ 4 Berichtigung, Sperrung und Löschung / Betroffenenrechte

(1) Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu sperren oder zu löschen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Sperrung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer wird den Auftraggeber nach Maßgabe der jeweils geltenden Datenschutzvorschriften mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person ("Betroffenenrechte") nachzukommen. Zu den Betroffenenrechten können insbesondere gehören:

- Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten;
- Recht auf Berichtigung, Löschung und Datenübertragbarkeit;
- Widerspruchsrecht und Recht auf nicht ausschließlich automatisierte Entscheidungsfindung im Einzelfall.

§ 5 Kontrollen und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestellt – soweit von den jeweils geltenden Datenschutzvorschriften vorgeschrieben – schriftlich einen Datenschutzbeauftragten. Name und Kontaktdaten des Datenschutzbeauftragten werden dem Auftraggeber unverzüglich nach Abschluss des Hauptvertrages schriftlich mitgeteilt, sofern dies nicht nachstehend angegeben ist:

(2)

Datenschutzbeauftragter des Auftragnehmers:
ADDAG GmbH & Co KG
Krefelder Strasse 121
52070 Aachen
Tel.: +49-241-44688-20; Fax: +49-241-44688-26
datenschutz@optilohn.de
Geschäftsführender Gesellschafter
Dr. Ralf W. Schadowski

Die Kontaktdaten des Datenschutzbeauftragten sind auf der Webseite des Auftragsnehmers einzusehen.

(2) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter bei der Aufnahme ihrer Tätigkeit gemäß den jeweils geltenden Datenschutzvorschriften auf das Datengeheimnis auch für die Zeit nach Beendigung dieser Vereinbarung verpflichtet wurden und in die Schutzbestimmungen der jeweils geltenden Datenschutzvorschriften eingewiesen worden sind.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen; Ermittlungen und Maßnahmen der datenschutzrechtlichen Aufsichtsbehörden.

(4) Der Auftragnehmer wird die Einhaltung der datenschutzrechtlichen Bestimmungen in seinem Verantwortungsbereich regelmäßig kontrollieren und gegebenenfalls erforderliche Anpassungen von Regelungen und/oder Maßnahmen zur Durchführung dieses Auftrags vornehmen.

(5) Der Auftragnehmer übermittelt dem Auftraggeber auf Wunsch des Auftraggebers schriftlich (a) Angaben über Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen, (b) Angaben über die Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung, (c) eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien, (d) Angaben über Empfänger oder Kategorien von Empfängern, denen die personenbezogenen Daten des Auftraggebers mitgeteilt werden können, (e) die Regelfristen für die Löschung der personenbezogenen Daten des Auftraggebers, (f) Hinweise auf eine geplante Datenübermittlung in Drittstaaten und (g) eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die technischen und organisatorischen Maßnahmen zur Gewährleistung eines entsprechenden Datenschutzniveaus getroffen wurden.

(6) Der Auftragnehmer wird ein den datenschutzrechtlichen Vorgaben entsprechendes Verzeichnis von Verarbeitungstätigkeiten ("Verfahrensverzeichnis") führen und dieses auf Anfrage der zuständigen Aufsichtsbehörde zur Verfügung stellen. Der Auftragnehmer wird den Auftraggeber über etwaige Anfragen der Aufsichtsbehörden unverzüglich informieren. Auskünfte an sonstige Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(7) Der Auftragnehmer wird den Auftraggeber nach Maßgabe der jeweils geltenden Datenschutzvorschriften bei einer etwaig erforderlichen Datenschutz-Folgenabschätzung und Konsultation mit den Aufsichtsbehörden unterstützen,

§ 6 Subunternehmer (Unterauftragsverhältnisse)

(1) Der Auftragnehmer darf bei der Datenverarbeitung die folgenden aktuellen Subunternehmer zu den jeweils genannten Leistungen einschalten:

- HS - Hamburger Software GmbH & Co KG, Überseering 29 in 22297 Hamburg
  Softwarehersteller der eingesetzten Lohnsoftware

- ALL-INKL.COM - Neue Medien Münnich, Inh. René Münnich
  Hauptstr. 68, 02742 Friedersdorf
  Webhosting und email-Provider

- H. Marc Rautenhaus, Eichenstrasse 5b in 52159 Roetgen
  IT-Dienstleister und Netzwerkadministrator

- Westwerk GmbH & Co KG, Charlottenstr. 14 in 52070 Aachen
  Webdesign und digitale Produkte; IT-Strategien

- Deutsche Post AG, Kundenservice E-Post in 33509 Bielefeld
  Maschinelle Einkuvertierung der Lohndokumente für den Postversand an den Arbeitnehmer

Eventuelle Änderungen der Subunternehmer werden auf der Webseite des Auftragnehmers dokumentiert.

(2) Der Auftragnehmer ist berechtigt, Subunternehmer zu beauftragen oder bereits beauftragte zu ersetzen. Der Auftragnehmer wird den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Subunternehmers informieren. Der Auftraggeber kann gegen eine beabsichtigte Änderung Einspruch erheben. Erhebt der Auftraggeber Einspruch, wird der Auftragnehmer den betroffenen Subunternehmer nicht beauftragen bzw. ersetzen.

(3) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, müssen die vertraglichen Vereinbarungen mit den Subunternehmern so gestaltet werden, dass sie den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages entsprechen. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend § 7 dieser Vereinbarung in diesen Verträgen mit den Subunternehmern in der Weise einzuräumen, dass sie den Auftraggeber, unbeschadet der Verantwortlichkeit des Auftragnehmers für die Subunternehmer, unmittelbar auch gegenüber den Subunternehmern berechtigen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf eine entsprechende Anforderung hin Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen durch die Subunternehmer zu erteilen.

(4) Der Auftragnehmer ist gegenüber dem Auftraggeber für sämtliche Handlungen und Unterlassungen der von Ihm eingesetzten Subunternehmer verantwortlich.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber kann sich nach Anmeldung zu Prüfzwecken in den Betriebsstätten des Auftragnehmers, in welchen die Verarbeitung der personenbezogenen Daten des Auftraggebers stattfindet, zu den üblichen Geschäftszeiten des Auftrag-

nehmers von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Datenschutzvorschriften überzeugen.

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben und die entsprechenden Nachweise gemäß § 3 Abs. 3 dieser Vereinbarung verfügbar zu machen, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

(2) Dem Auftragnehmer sind die geltenden datenschutzrechtlichen Melde- bzw. Benachrichtigungspflichten gegenüber Aufsichtsbehörden und Betroffenen, insbesondere deren zeitliche und inhaltliche Vorgaben, bekannt. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers.

(3) Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Melde- bzw. Benachrichtigungspflichten treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

(4) Der Auftragnehmer hat etwaige Verstöße, einschließlich aller hiermit im Zusammenhang stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen, entsprechend der jeweils geltenden Datenschutzvorschriften zu dokumentieren. Die Dokumentation ist dem Auftraggeber auf Aufforderung unverzüglich herauszugeben.

§ 9 Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(2) Soweit Weisungen des Auftraggebers Ermessensspielräume enthalten sollten, ist der Auftragnehmer verpflichtet, hierzu die Entscheidung des Auftraggebers einzuholen. Eine eigenständige Ermessensausübung oder Kulanzentscheidung steht dem Auftragnehmer nicht zu.

(3) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben oder ohne eine entsprechende, ausdrückliche und schriftliche Weisung des Auf-

traggebers an Stellen außerhalb der Mitgliedsstaaten des Europäischen Wirtschaftsraumes übermitteln. Kopien und Duplikate 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.

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

§ 10 Löschung von Daten und Rückgabe von Datenträgern

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte 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.

(2) 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 Auftragnehmer außerhalb der EU

(1) Sofern die Verarbeitung personenbezogener Daten außerhalb der EU erfolgt, garantiert der Auftragnehmer, dass die nach den jeweils geltenden Datenschutzvorschriften anwendbaren Voraussetzungen für das Eingreifen eines Erlaubnistatbestandes für die Verarbeitung personenbezogener Daten außerhalb der EU erfüllt sind ("datenschutzrechtliche Rechtfertigung").

(2) Der Auftragnehmer garantiert dem Auftraggeber hinsichtlich der datenschutzrechtlichen Rechtfertigung konkret, dass

- eine Verarbeitung der personenbezogenen Daten außerhalb der EU erfolgt nicht.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, sofern die datenschutzrechtliche Rechtfertigung nicht mehr eingreift und/oder für ihn erkennbar ist, dass die datenschutzrechtliche Rechtfertigung vor Ende des Auftrages nicht mehr eingreifen wird.

(4) Der Auftragnehmer stellt den Auftraggeber von sämtlichen Ansprüchen Dritter frei, die davon herrühren, dass

- die datenschutzrechtliche Rechtfertigung aufgrund eines vom Auftragnehmer zu vertretenen Umstandes nicht mehr eingreift, und/oder

- der Auftragnehmer den Auftraggeber nicht rechtzeitig über den Wegfall der datenschutzrechtlichen Rechtfertigung informiert hat.

Die Freistellungsverpflichtung umfasst insbesondere auch etwaige Buß- und Ordnungsgelder sowie die angemessenen Rechtsanwaltskosten des Auftraggebers.

(5) Sofern die jeweilige datenschutzrechtliche Rechtfertigung wegfällt, kann der Auftraggeber nach freiem Ermessen entweder

- den Hauptvertrag unmittelbar außerordentlich kündigen oder

- den Auftragnehmer mit Fristsetzung zum Nachweis einer anderen datenschutzrechtlichen Rechtfertigung oder zum Abschluss von Standardvertragsklauseln auffordern, die den Anforderungen der für den Auftraggeber zuständigen Datenschutzbehörde entsprechen, wobei der Auftragnehmer die im Zusammenhang mit dem Nachweis anfallenden Kosten zu tragen hat. Kommt der Auftragnehmer dieser Aufforderung nicht fristgerecht nach, kann der Auftraggeber den Hauptvertrag ebenfalls außerordentlich kündigen.

(6) Im Falle der außerordentlichen Kündigung hat der Auftragnehmer dem Auftraggeber auf dessen Wunsch auf eigene Kosten dabei zu unterstützen, dass die personenbezogenen Daten unverzüglich an einen anderen, vom Auftraggeber benannten Auftragnehmer übergeben werden können.

(7) Sofern die Verarbeitung personenbezogener Daten außerhalb der EU erfolgt garantiert der Auftragnehmer weiterhin, dass er für die Laufzeit des Auftrages ununterbrochen einen im Inland ansässigen Vertreter benannt hat, sofern dies nach den jeweils geltenden Datenschutzvorschriften erforderlich ist. Der Vertreter ist beauftragt, zusätzlich zum Auftragnehmer oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung der datenschutzrechtlichen Vorschriften als Anlaufstelle zu dienen.

§ 12 Kosten

(1) Der Auftragnehmer trägt alle Kosten, welche Ihm durch die Erfüllung der in dieser Vereinbarung vorgesehenen Verpflichtungen entstehen.

(2) Die Parteien sind sich einig, dass der Auftragnehmer auch für die Erfüllung der in dieser Vereinbarung geregelten Verpflichtungen durch die in dem Hauptvertrag vorgesehene Vergütung entlohnt wird und dass der Auftragnehmer im Hinblick auf diese Vereinbarung keine darüber hinausgehende Vergütung erhält.

§ 13 Sonstiges, Allgemeines

(1) Sollten die personenbezogenen 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 zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den personenbezogenen Daten des Auftraggebers bei dem Auftraggeber liegt.

(2) Unbeschadet des Weisungsrechts des Auftraggebers gemäß § 9 dieser Vereinbarung bedürfen Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Die Regelungen dieser Vereinbarung gelten auch nach einer Beendigung des Hauptvertrages bis zur vollständigen Vernichtung oder Rückgabe aller personenbezogenen Daten des Auftraggebers an den Auftraggeber fort.

(4) Im übrigen gelten die Bestimmungen des Hauptvertrages entsprechend.

_____ _____

(Ort, Datum) (Unterschrift Auftraggeber)

_____

(Unterschrift Auftragnehmer)

Anhang 1: Datenschutz- und Sicherheitskonzept

Anlage – Technisch-organisatorische Maßnahmen

Diese stellt der Auftragnehmer dem Auftraggeber in freier Form zur Prüfung zur Verfügung.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie

Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.