Vereinbarung zur Auftragsdatenverarbeitung

Die Vertragsparteien

_____
Unternehmensbezeichnung, Firma

_____
Straße, Hausnummer

_____
PLZ, Ort

- im Folgenden: Auftraggeber -

und

Horst Klaes GmbH & Co. KG
Wilhelmstr. 85-87
53474 Bad Neuenahr-Ahrweiler
Deutschland

- im Folgenden: Auftragnehmer -

schließen folgenden Vertrag:

Präambel

Diese Bedingung beschreibt die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den Verträgen der Parteien ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit einem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten. Eine Beschreibung der Datenarten, Betroffenen und Kategorien von Empfängern sowie der Auftragsverarbeitungstätigkeit ist diesem Vertrag unter Punkt 1.1 dargestellt.

1. Gegenstand des Auftrags, Begriffsbestimmung

1.1. Gegenstand des vorliegenden Vertrags ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (im Folgenden „Daten“) durch den Auftragnehmer, die diesem durch den Auftraggeber zum Zwecke der Durchführung des Vertrags vom _____ *(hier Datum des Hauptvertrags mit dem Auftragnehmer)* - im Folgenden: „Hauptvertrag“ - überlassen werden.

Der vorliegende Vertrag umfasst folgende Leistungen:

- Zugriff per Fernwartungstool des Auftragnehmers auf das Datenverarbeitungssystem des Auftraggebers zum Zweck der Remote-Hilfestellung, Fehlerbeseitigung, Beratung o.ä. nach Freigabe durch den Auftraggeber
- Überprüfung der Daten des Auftraggebers in Bezug auf Fehler in den Daten oder der verwendeten Software des Auftraggebers in den Räumlichkeiten des Auftragnehmers
- Protokollierung des Auftragnehmers der Kontakte, Gespräche, Leistungen, Tätigkeiten mit den Auftraggebern Versand von Waren an den Auftraggeber
- Verwaltung diverser Auftraggeber-Zugangsdaten zu Systemen des Auftraggebers, wie z.B. Benutzeranmeldedaten
- Nennung des Auftraggebers auf den Internetauftritten und in Marketingmaterialien des Auftragnehmers als Referenzen nach Zustimmung des Auftraggebers
- Verwaltung von E-Mailadressen des Auftraggebers und dessen Mitarbeitern zur Zusendung von Mails, Newslettern etc. nach deren expliziter Zustimmung

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgenden Datenarten verarbeitet:

- Anschrift und Name des Auftraggebers
- Namen, geschäftliche Telefonnummern, E-Mailadressen, Position im Unternehmen und Benutzer-Accounts der Mitarbeiter des Auftraggebers
- Wenn vorhanden und benötigt, IP-Adressen des Auftraggebers
- Datensicherung des Auftraggebers inkl. evtl. Drittadressen

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

- Alle Mitarbeiter des Auftragnehmers

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:

- Per gesicherter Fernverbindung auf die DV-Systeme des Auftraggebers
- Daten des Auftraggebers werden vom Auftragnehmer über ein verschlüsseltes, portables Medium gesichert; persönlich oder per Paketdienst an den Auftragnehmer gebracht und dort auf gesicherte und verschlüsselte Systeme des Auftragnehmers übertragen
- Daten können durch den Auftraggeber auf einen geschützten FTP-Server des Auftragnehmers übertragen werden. Diese werden dann vom Auftragnehmer auf gesicherte und verschlüsselte DV-Systeme kopiert

1.2. Der Auftraggeber hat den unterzeichnenden Auftragnehmer sorgfältig und gewissenhaft und im Einklang mit den bestehenden gesetzlichen Vorschriften – insbesondere unter Beachtung seiner gesetzlichen Pflichten – ausgewählt.

1.3. Die Auftragsdatenverarbeitung darf nicht vor Abschluss der schriftlichen Auftragserteilung des Auftraggebers gegenüber dem Auftragnehmer beginnen, die durch den vorliegenden Vertrag erfolgt.

1.4. Die vom Auftraggeber überlassenen Daten dürfen vom Auftragnehmer ausschließlich zur Erfüllung des vereinbarten Vertragszwecks verarbeitet, erhoben oder genutzt werden.

1.5. Die Erhebung, Nutzung und Verarbeitung der Daten durch den Auftragnehmer findet

- ausschließlich in Deutschland
- in den Mitgliedstaaten der Europäischen Union (EU) bzw. im Gemeinsamen Europäischen Wirtschaftsraum (EWR)

statt. Sollte der Auftragnehmer Unterauftragnehmer in einem Drittland (Nicht-EU bzw. Nicht-EWR) mit der Datenverarbeitung beauftragen, darf dies nicht ohne schriftliche Einwilligung des Auftraggebers erfolgen. Darüber hinaus hat er für ein angemessenes Datenschutzniveau zu sorgen und sicherzustellen, dass alle gesetzlichen (insbesondere nach dem BDSG, der EU-DSGVO und den Landesdatenschutzgesetzen) und vertraglichen Pflichten eingehalten werden.

2. Dauer des Auftrags und Kündigung

2.1. Der Vertrag beginnt mit der Unterzeichnung der vorliegenden Vereinbarung – nicht jedoch vor Unterzeichnung und Wirksamkeit des Hauptvertrages – und endet

- mit der Beendigung des Hauptvertrages
- mit Kündigung

Die Parteien sind sich darüber im Klaren, dass die Auftragsdatenverarbeitung nicht ohne einen gültigen Vertrag über die Verarbeitung personenbezogener Daten im Auftrag erfolgen darf, sodass die Auftragsdatenverarbeitung im Falle der Beendigung des vorliegenden Vertrages bis zum Abschluss eines neuen Vertrages über die Verarbeitung personenbezogener Daten im Auftrag nicht erfolgend darf.

2.2. Eine ordentliche Kündigung dieses Vertrages ist ausgeschlossen. Das Vertragsverhältnis über die Verarbeitung personenbezogener Daten im Auftrag endet automatisch mit der Beendigung des entsprechenden Hauptvertrages.

2.3. Das Recht zur fristlosen Kündigung bleibt von den vorliegenden Ziffern unberührt. Ein Recht zur fristlosen Kündigung ist insbesondere im Falle von schweren, vorsätzlichen und/oder wiederholten Verstößen gegen vertragliche oder gesetzliche Datenschutzbestimmungen gegeben. Ein schwerer Verstoß liegt insbesondere vor, wenn der Auftragnehmer den Weisungen des Auftraggebers – gleich aus welchem Grund – nicht nachkommt oder Kontrollen durch den Auftraggeber oder die zuständigen Aufsichtsbehörden nicht unterstützt, behindert oder erschwert.

3. Allgemeine Pflichten des Auftragsnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und

Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Die Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass ein angemessenes oder vertraglich vereinbartes Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Dieser Aufwand wird dem Auftragnehmer vom Auftraggeber zu den jeweils geltenden Stundensätzen des Auftragnehmers vergütet.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet durch regelmäßige Audits, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der
technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe; Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(11) Die vorstehend geschilderten Aufwände sind vom Auftraggeber an den Auftragnehmer zu dessen jeweils gültigen Preisen gemäß Preisliste zu vergüten.

4. Technische und organisatorische Maßnahmen

4.1. Der Auftragnehmer verpflichtet sich dazu, technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu treffen. Die einzelnen, zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen, ergeben sich aus Anlage 2 zu diesem Vertrag.

4.2. Der Auftragnehmer wird die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig überprüfen und ggf. optimieren.

4.3. Die Parteien sind sich darüber einig, dass die technischen und organisatorischen Maßnahmen aufgrund rechtlicher, technischer oder tatsächlicher Änderungen ggf. modifiziert werden müssen. Hierbei sind wesentliche Änderungen, durch die datenschutzrechtliche Belange beeinträchtigt werden können, mit dem Auftraggeber abzustimmen. Andere Maßnahmen, durch die keine Einschränkung datenschutzrechtlicher Belange zu befürchten ist, können vom Auftragnehmer auch ohne Abstimmung vorgenommen werden. In jedem Fall ist dem Auftraggeber auf Anfrage jederzeit eine aktuelle Auflistung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen vorzulegen.

5. Datengeheimnis

5.1. Der Auftraggeber weist den Auftragnehmer ausdrücklich auf die gesetzlichen Bestimmungen zum Datengeheimnis hin. Der Auftragnehmer hat dafür Sorge zu tragen, dass alle Personen, die von ihm zur Verarbeitung der vertragsgegenständlichen personenbezogenen Daten eingesetzt werden, ausdrücklich zu gesetzlich vorgeschriebenen Geheimhaltungspflichten verpflichtet und über die besonderen Weisungs- und Zweckbindungen sowie gegebenenfalls besonderen Datenschutz- oder Geheimhaltungspflichten belehrt werden. Der Auftragnehmer wird die genannten Personen auch auf die Geheimhaltungsregeln nach § 203 StGB (Verletzung von Privatgeheimnissen) und § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen) hinweisen. Die vorgenannten Personen werden vom Auftragnehmer ferner darauf hingewiesen, dass die entsprechenden Verpflichtungen grundsätzlich auch nach der Beendigung der Tätigkeit fortbestehen.

5.2. Der Auftragnehmer versichert, dass ihm und allen von ihm zur Erfüllung des vorliegenden Vertrags eingesetzten Personen die geltenden datenschutzrechtlichen Vorschriften und deren Anwendung bekannt sind.

5.3. Gesetzliche Offenbarungspflichten des Auftragnehmers bleiben von den vorgenannten Regelungen unberührt.

6. Mitteilungs- und Dokumentationspflichten des Auftragnehmers

6.1. Der Auftragnehmer verpflichtet sich, jeden Verstoß gegen datenschutzrechtliche Bestimmungen, gegen diesen Vertrag und/oder die Weisungen des Auftraggebers unverzüglich mitzuteilen. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer bei ihm angestellten Person, einem Unterauftragnehmer oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten gegenüber dem Auftragnehmer eingesetzt hat, begangen wurde. Der Auftragnehmer ist insbesondere verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten zu unterstützen.

6.2. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten Daten betroffen sein könnten.

6.3. Sollten die dem Auftragnehmer vom Auftraggeber überlassenen Daten im Rahmen dieses Vertrages durch ein Insolvenzverfahren, eine Pfändung, eine Beschlagnahme, ein Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gegenüber dem Auftragnehmer gefährdet sein, hat der Auftragnehmer den Auftraggeber unverzüglich hierüber zu informieren. Der Auftraggeber hat daraufhin die für die Maßnahme verantwortlichen Personen darüber zu informieren, dass das Eigentum bzw. die Inhaberschaft und sämtliche Rechte an den Daten bei ihm als verantwortliche Stelle im Sinne des Gesetzes liegen.

6.4. Der Auftragnehmer verpflichtet sich ferner, sämtliche Weisungen des Auftraggebers schriftlich oder in einer anderen geeigneten Form zu dokumentieren und dem Auftraggeber alle Verzeichnisse, Protokolle und weitere erforderliche Informationen zum Nachweis der Einhaltung gesetzlicher Pflichten auf Anforderung unverzüglich zur Verfügung zu stellen und Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und in angemessener Weise dazu beizutragen.

7. Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO gilt § 2 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

8. Kontrollbefugnisse des Auftraggebers

8.1. Der Auftraggeber ist berechtigt und verpflichtet, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Schutz personenbezogener Daten vor Beginn der Datenverarbeitung und sodann während der Vertragslaufzeit regelmäßig und jederzeit im erforderlichen Umfang zu kontrollieren. Von dieser Kontrollbefugnis sind insbesondere die Einhaltung der Weisungen des Auftraggebers, die Erfüllung der gesetzlichen Protokoll- und Dokumentationspflichten und die Verwirklichung der erforderlichen technischen und organisatorischen Maßnahmen umfasst. Auf Verlangen des Auftraggebers hat der Auftragnehmer zudem Einsicht in die vom Auftragnehmer zur Durchführung des Auftrags verwendeten Datenverarbeitungsprogramme bzw. -systeme zu ermöglichen.

8.2. Der Auftragnehmer hat grundsätzlich sämtliche Kontroll- und Aufsichtsmaßnahmen in angemessenem Umfang zu unterstützen und zu dulden. Er ist gegenüber dem Auftraggeber insbesondere zur vollständigen und wahrheitsgemäßen Auskunftserteilung verpflichtet, soweit dies für die Durchführung der in dieser Ziffer genannten Kontrollen erforderlich ist.

8.3. Im Rahmen der vorgenannten Kontrollen sind Störungen des Betriebsablaufs des Auftragnehmers so weit wie möglich zu vermeiden. Insbesondere sollen Besichtigungen der Betriebsstätte des Auftragnehmers in der Regel mit einer angemessenen Vorlauffrist

angekündigt werden und zu den jeweils üblichen Geschäftszeiten vorgenommen werden, sofern dies dem Erfolg der Kontrollmaßnahme nicht entgegensteht. Steht der Verdacht eines Verstoßes gegen gesetzliche oder vertragliche Datenschutzbestimmungen im Raum, kann die Kontrolle – inklusive der Betriebsbesichtigung – ohne Voranmeldung erfolgen, wobei auf die Verhältnismäßigkeit der Kontrollmaßnahme zu achten ist.

8.4. Im Falle von Unregelmäßigkeiten bei der Datenverarbeitung wird der Auftraggeber den Auftragnehmer unverzüglich informieren und geeignete Maßnahmen ergreifen bzw. Weisungen erteilen, um den Verstoß schnellstmöglich abzustellen.

8.5. Der Auftraggeber und der Auftragnehmer dokumentieren die Ergebnisse der Kontrollen eigenständig.

9. Weisungsbefugnis des Auftraggebers

9.1. Der Auftraggeber behält sich vor, den Auftragsgegenstand nach Art, Umfang und Verfahren im Rahmen dieser Vereinbarung durch mündliche oder schriftliche Weisungen zu konkretisieren. Im Falle einer mündlichen Weisung ist diese unverzüglich schriftlich durch den Auftraggeber zu bestätigen. Der Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren. Der Auftraggeber hat ausdrücklich den Grund dafür zu benennen, warum keine schriftliche Weisung erfolgen konnte.

9.2. Änderungen des Vertragsgegenstandes müssen gemeinsam mit dem Auftragnehmer abgestimmt werden.

10. Berichtigung, Löschung und Sperrung der Daten

10.1. Nicht mehr benötigte personenbezogene Daten oder Unterlagen dürfen nur mit Zustimmung des Auftraggebers berichtigt, gesperrt oder vernichtet werden. Im Übrigen kann der Auftraggeber vor, während oder nach Beendigung der Vertragslaufzeit die Berichtigung, Löschung, Sperrung oder Herausgabe der Daten verlangen. Der Auftragnehmer hat einer entsprechenden Weisung unverzüglich Folge zu leisten.

10.2. Ersucht ein Betroffener den Auftragnehmer um Berichtigung, Löschung, Sperrung oder Einsicht von Daten, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung von dessen Pflichten ggü. den Betroffenen unterstützen.

11. Einsatz von Unterauftragnehmern (Subunternehmer)

11.1. Der Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zum Einsatz von Unterauftragnehmern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und seitens des Auftraggebers ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 1 beigefügt. Für die in Anlage 1 aufgezählten Subunternehmer gilt die schriftliche Einwilligung mit Unterzeichnung dieses Vertrags als erteilt.

11.2. Die Handlungen des Unterauftragnehmers, die mit der Vertragsdurchführung in Zusammenhang stehen, werden dem Auftragnehmer wie eigene Handlungen zugerechnet.

11.3. Der Auftragnehmer versichert, dass er seine Unterauftragnehmer sorgfältig und gewissenhaft ausgewählt hat und zukünftige Unterauftragnehmer entsprechend auswählen wird, sodass deren Einsatz die ordnungsgemäße Vertragsdurchführung im Verhältnis zum

Auftraggeber nicht beeinträchtigt. Insbesondere stellt er durch geeignete vertragliche Regelungen und entsprechende Unterauftragsdatenverarbeitungsverträge sicher, dass der Subunternehmer die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer hat zudem sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragnehmer regelmäßig kontrolliert und dokumentiert.

11.4. Der Auftragnehmer hat sich von seinen Unterauftragnehmern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen betrieblichen Datenschutzbeauftragten bestellt haben. Wenn kein Datenschutzbeauftragter bestellt wurde oder ein solcher während der Vertragslaufzeit ersatzlos ausscheidet, ist der Auftraggeber vom Auftragnehmer über diesen Umstand zu unterrichten.

11.5. Sämtliche Verträge zwischen Auftragnehmer und Unterauftragnehmer (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den Anforderungen der gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber den Unterauftragnehmern ausgeübt werden können.

11.6. Der Auftragnehmer ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragnehmers einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.

11.7. Dienstleistungen, die der Auftragnehmer als reine Nebenleistungen zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, sind nicht als Unteraufträge im Sinne dieser Ziffer anzusehen. Hiervon umfasst sind z.B. Reinigungsleistungen, Telekommunikationsdienstleistungen, die keinen konkreten Bezug zur vertragsgegenständlichen Leistung aufweisen sowie Post- und Kurierdienste, sonstige Transportleistungen und Bewachungsdienste. Auch im Falle nicht zustimmungsbedürftiger Nebenleistungen muss der Auftragnehmer die erforderlichen organisatorischen und technischen Vorkehrungen zum Schutz personenbezogener Daten treffen. Gesetzlich vorgeschriebene Wartungs- und Prüfungsdienstleistungen gelten als zustimmungsbedürftige Unteraufträge, sofern

hiervon diejenigen IT-Systeme umfasst sind, die auch zur Erbringung der vertragsgegenständlichen Leistung genutzt werden.

11.8. Sollte der Auftragnehmer Unterauftragnehmer in einem Drittland (Nicht- EU bzw. Nicht-EWR) mit der Datenverarbeitung beauftragen wollen, darf dies nicht ohne schriftliche Einwilligung des Auftraggebers erfolgen. Über die in den vorangegangenen Ziffern genannten Pflichten hinaus hat er für ein angemessenes Datenschutzniveau zu sorgen und sicherzustellen, dass alle gesetzlichen und vertraglichen Pflichten eingehalten werden.

12. Rückgabe und Löschung der Daten und Datenträger nach Vertragsbeendigung

12.1. Nach Vertragsbeendigung ist der Auftragnehmer verpflichtet, sämtliche im Zusammenhang mit dem Auftrag erlangten Datenbestände, Nutzungs- und Verarbeitungsergebnisse sowie Datenträger an den Auftraggeber auszuhändigen und/oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial sowie ggf. beim Auftraggeber verbliebene Datensicherungen. Der

Auftragnehmer hat die Vernichtung der Daten in geeigneter Weise zu protokollieren.

12.2. Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragnehmers nach Absatz 1 in geeigneter Weise zu kontrollieren. Hierzu ist er insbesondere berechtigt, die Protokolle über die Vernichtung der Daten einzusehen, sowie die betreffenden Datenverarbeitungsanlagen und die Betriebstätte des Auftragnehmers in Augenschein zu nehmen. Die Besichtigung der Betriebsstätte soll zu den regulären Geschäftszeiten erfolgen und ist ggü. dem Auftragnehmer rechtzeitig anzukündigen, sofern dies den Erfolg der Kontrollmaßnahme nicht gefährdet.

12.3. Von der Löschungspflicht werden der Schriftwechsel und die nach den gesetzlichen Vorschriften aufzubewahrenden Dokumente oder Vertragsunterlagen oder sonstige für den Auftragnehmer bestimmte Unterlagen nicht erfasst. Für diese Dokumente gelten die ggf. einschlägigen Aufbewahrungsfristen. Weitergehende Löschungsansprüche bleiben von der vorliegenden Ziffer unberührt.

13. Schlussbestimmungen

13.1. Der Auftragnehmer verzichtet hinsichtlich der ihm zum Zwecke der Vertragsdurchführung überlassenen Daten und Datenträger auf sein Zurückbehaltungsrecht.

13.2. Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen Vereinbarung, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll. Dies gilt auch für den Verzicht auf das Schriftformerfordernis.

13.3. Sollten einzelne Regelungen dieses Vertrags unwirksam sein, bleibt der Rest dieser Vereinbarung hiervon unberührt.

13.4. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

13.5. Erfüllungsort und Gerichtsstand ist Bad Neuenahr-Ahrweiler.

_____, den _____
Ort Datum

Unterschrift (Auftraggeber)

Horst Klaes GmbH & Co. KG,
Markus Klaes

ppa.

Unterschrift (Auftragnehmer)

Anlage 1 – Bestehende Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Unternehmens-) Name und Anschrift	Beschreibung der Leistung	Ort der Leistungserbringung
TERRA CLOUD GmbH Hankamp 2 32609 Hüllhorst	Wenn vom AG beauftragt Betrieb von virtualisierten Servern der AG Hosten der Datensicherungen der AG	32609 Hüllhorst
SolarWinds Worldwide Unit 1101, Building 1000 City Gate, Mahon Cork Irland	Wenn vom AG beauftragt Monitoring von DV-Anlagen der AG Hosten der Datensicherungen der AG	Düsseldorf
Deutsche Post AG Charles-de-Gaulle-Straße 20 53113 Bonn	Versand von Briefen und Paketen	Deutschlandweit
DHL Paket GmbH Sträßchensweg 10 53113 Bonn	Versand von Briefen und Paketen	Deutschlandweit
UPS Europe SA Ave Ariane 5 B-1200 Brüssel Belgien	Versand von Briefen und Paketen	Weltweit
Vodafone GmbH Ferdinand-Braun-Platz 1 40549 Düsseldorf	Herstellung von Telefon- und Internetverbindung	Weltweit
united-domains AG Gautinger Straße 10 82319 Starnberg	Domainverwaltung sowie IP Weiterleitungen an die Server des AN	Deutschland
ELO Digital Office GmbH Tübinger Str. 43 70178 Stuttgart	Wenn vom AG beauftragt Lieferung und Wartung deren Software	Stuttgart
combit Software GmbH Untere Laube 30 78462 Konstanz	Wenn vom AG beauftragt Lieferung und Wartung deren Software	Konstanz
CAD Line Hard- und Software Vertriebs GmbH Wieteleck 4 32549 Bad Oeynhausen	Wenn vom AG beauftragt Lieferung und Wartung deren Software	Bad Oeynhausen
Compass Software GmbH Steinhammerstraße 140a 44379 Dortmund	Wenn vom AG beauftragt Lieferung und Wartung deren Software	Dortmund
Sophos Ltd Abingdon Science Park Abingdon OX14 3YP Vereinigtes Königreich	Wenn vom AG beauftragt Lieferung und Wartung deren Antimalwarelösungen	Deutschland und UK
PAV Germany GmbH Dr.-Alfred-Herrhausen-Allee 26 47228 Duisburg	Wenn vom AG beauftragt Lieferung und Wartung deren Antimalwarelösungen	Deutschland und Spanien

Anlage 2 – Technische und organisatorische Maßnahmen im Sinne von Art. 32 DSGVO

Maßnahmen die geeignet sind, Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle).
Es existieren folgende Maßnahmen zur Zutrittskontrolle:

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

Maßnahmen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle).
Es existieren folgende Maßnahmen zur Zugangskontrolle:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername/Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Sperren von externen Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von zentraler Smartphone-Administrations-Software
- (z.B. zum externen Löschen von Daten)
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops/Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

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 (Zugriffskontrolle).
Es existieren folgende Maßnahmen zur Zugriffskontrolle:

- 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
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung

- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

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 (Weitergabekontrolle).
Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- 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
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –Fahrzeugen

Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).
Es existieren folgende Maßnahmen zur Eingabekontrolle:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle).
Es existieren folgende Maßnahmen zur Auftragskontrolle:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vertragsstrafen bei Verstößen

Maßnahmen die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).
Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung

- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen

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

Es existieren folgende Maßnahmen zur Trennungskontrolle:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten