Auftragsverarbeitung

Auftragsverarbeitung nach Art. 28 Abs. 3 der Verordnung (EU) 2016/679
(EU Datenschutz-Grundverordnung, DSGVO)

gripsware (für die Zwecke dieses Dokuments auch als „**Auftragnehmer**“ bezeichnet) übernimmt als Auftragsverarbeiter i.S. von Art. 28 Abs. 3 DSGVO gegenüber dem Kunden als „Verantwortlichem“ i.S.d. Art. 4 Nr. 7 DSGVO (für die Zwecke dieses Dokuments auch als „**Auftraggeber**“ bezeichnet) die nachfolgenden Pflichten mit den nachfolgenden Rechten, wenn und soweit die Leistungen des Auftragnehmers nach dem mit dem Auftraggeber geschlossenen Vertrag unter der an den Auftraggeber als Kunden vergebenen Kundennummer („**Hauptvertrag**“) auch eine Verarbeitung personenbezogener Daten im Auftrag und auf Weisung des Auftraggebers umfasst. Dieses vorliegende Dokument („**AVV**“) ist integraler Bestandteil des Vertragswerks.

1. Gegenstand, Grundsätzliches und Dauer der Vereinbarung

1.1 Nach dem Inhalt des Hauptvertrags über die Leistungen des Auftragnehmers und nach den vom Auftraggeber vorgenommenen Nutzungen ist es nicht ausgeschlossen, dass der Auftragnehmer dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO verarbeitet und der Auftragnehmer dabei keine eigenen Zwecke im Umgang mit diesen Daten des Auftraggebers verfolgt. Wenn dies geschieht, so erfolgt diese Verarbeitung von personenbezogenen Daten des Auftraggebers im Auftrag und auf Weisung für die Zwecke des Auftraggebers nach Maßgabe dieses Vertrags.

1.2 „**Anlage 1 zur Auftragsverarbeitung - Individuelle Vertragsbestandteile**“ enthält die für den Auftragnehmer maßgeblichen Weisungen des Auftraggebers zur Konkretisierung der Auftragsverarbeitungsleistungen.

1.3 „**Weisung**“ ist die auf einen bestimmten datenschutzmäßigen Umgang des Auftragnehmers mit personenbezogenen Daten, die der Auftraggeber verarbeitet, gerichtete Anordnung des Auftraggebers (z.B. Daten zu anonymisieren, zu sperren, zu löschen, herauszugeben). Bereits bestehende Weisungen können vom Auftraggeber danach durch einzelne Weisungen geändert, ersetzt oder ergänzt werden (Einzelweisungen). Die Parteien beachten dabei Ziff. 3.2 und 3.3 dieser AVV.

1.4 Der Auftraggeber ist für die Beurteilung der Zulässigkeit der Verarbeitung personenbezogener Daten durch den Auftragnehmer auf IT-Systemen des Auftraggebers, IT-Systemen des Auftragnehmers sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Der Auftraggeber hat dafür Sorge zu tragen, dass die gesetzlich oder behördlich vorgeschriebenen Voraussetzungen für „seine“ Datenverarbeitungen geschaffen werden bzw. Anforderungen erfüllt werden, wie z.B. die Definition und Einhaltung von Löschfristen und zulässiger Speicherdauer oder die Einholung von ggfs. erforderlichen Einwilligungserklärungen. Das gilt insbesondere dann, wenn der Auftraggeber besonders sensible Daten im Sinne des Art. 9 DSGVO verarbeiten lässt.

1.5 Der Auftraggeber stellt den Auftragnehmer in seinem Verantwortungsbereich von Ansprüchen Betroffener gegenüber dem Auftragnehmer frei. Art. 82 DSGVO bleibt unberührt.

1.6 Gegenstand, Dauer, Art und Zweck der Datenverarbeitung im Auftrag ist durch den Hauptvertrag zwischen den Parteien vorgegeben, der zivilrechtlich die Leistungserbringung regelt, sowie den zugehörigen jeweiligen Leistungsbeschreibungen und ggf. mitgeltenden Dokumenten.

1.7 Im Rahmen der produktspezifischen Möglichkeiten der vom Hauptvertrag umfassten Leistungen bzw. Produkte des Auftragnehmers kann der Auftraggeber Art und Umfang seiner Datenverarbeitung durch Art und Weise der Nutzung des Produktes bestimmen.

Im Rahmen dieser Produkte können dann insbesondere Weisungsrechte des Auftraggebers im Falle der Inanspruchnahme von Gewährleistung, Pflegeleistungen oder im Einzelfall gewünschten Serviceleistungen wie z.B. eine Programmierung wahrgenommen werden, wenn der Auftragnehmer im Einzelfall auf den Datenbestand des Auftraggebers Zugriff nehmen soll.

1.8 Sämtliche Auftragsverarbeitungsleistungen des Auftragnehmers werden ausschließlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) erbracht. Jede Verlagerung dieser Auftragsverarbeitungsleistungen oder von Teilen davon in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. ein Angemessenheitsbeschluss der Kommission vorliegt, Standarddatenschutzklauseln verwendet werden oder genehmigte Verhaltensregeln vorliegen).

1.9 Diese AVV beginnt mit dem Zustandekommen des Hauptvertrags und wird auf unbestimmte Zeit geschlossen. Die AVV endet mit dem Ende der vertraglich vereinbarten Leistungen des Auftragnehmers aus dem Hauptvertrag. Klarstellend wird festgehalten, dass dieser Zeitpunkt auch nach dem Ende der Laufzeit des Hauptvertrags liegen kann und die AVV in jedem Fall so lange gültig bleibt, wie der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

1.10 Der Auftraggeber kann die AVV jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder gegen die Bestimmungen der AVV vorliegt, der Auftragnehmer eine Weisung des Auftraggebers schuldhaft nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

In diesem Fall ist der Hauptvertrag entsprechend anzupassen, insbesondere besteht bei Leistungen, die nur unter Geltung der AVV oder einer vergleichbaren Vereinbarung zulässig sind, erst dann wieder eine Leistungspflicht des Auftragnehmers, wenn eine neue AVV oder eine mit der AVV vergleichbare Vereinbarung abgeschlossen wurde, oder die Parteien sich einigen, betreffende Leistungen aus dem Leistungsumfang des Hauptvertrag herauszunehmen. Können sich die Parteien nicht binnen angemessener Frist einigen, ist jede der Parteien zur außerordentlichen Kündigung auch des Hauptvertrags berechtigt, ohne dass der anderen Partei deshalb Ersatzansprüche zustehen.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Die Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO), der Zweck der Verarbeitung, die Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO) sowie die Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO) ergeben sich aus „**Anlage 1 zur Auftragsverarbeitung - Individuelle Vertragsbestandteile**“.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

3.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO 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.

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

3.3 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. Als Bestätigung gilt auch der widerspruchslose Zugang einer solchen Bestätigung des Auftragnehmers beim Auftraggeber.

3.4 Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

3.5 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen. Die Regelung im Hauptvertrag zum Umgang mit vertraulichen Informationen gilt insofern entsprechend.

3.6 Bei speziellen Weisungen, deren Umsetzung für den Auftragnehmer nicht oder nur mit unverhältnismäßig hohem Mehraufwand möglich ist, kann der Auftragnehmer den Hauptvertrag und diesen Auftragsverarbeitungsvertrag zum Ende eines laufenden Kalendermonats mit einer Frist von zwanzig (20) Kalendertagen kündigen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

4.1 Weisungsberechtigte Personen des Auftraggebers und Weisungsempfänger des Auftragnehmers sind in „**Anlage 1 zur Auftragsverarbeitung - Individuelle Vertragsbestandteile**“ enthalten.

4.2 Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

5. Pflichten des Auftragnehmers

5.1 Der Auftragnehmer verarbeitet personenbezogene Daten in der Situation der Auftragsverarbeitung 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, verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber 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 DSGVO).

5.2 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen Zwecke, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftraggeber wird ausdrücklich darauf hingewiesen, dass solche Kopien oder Duplikate im Zusammenhang mit den Datensicherungen entstehen können, die der Auftragnehmer im ordentlichen Geschäftsgang anfertigt. Siehe dazu auch „**Anlage 2 zur Auftragsverarbeitung - Technische und organisatorische Maßnahmen**“.

5.3 Der Auftragnehmer gewährleistet im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen. Er gewährleistet durch geeignete technisch-organisatorische Maßnahmen, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

5.4 Die Datenträger, die vom Auftraggeber stammen bzw. die ausschließlich für den Auftraggeber genutzt werden, werden besonders gekennzeichnet.

5.5 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO 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 DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Weisungsberechtigten des Auftraggebers gemäß „**Anlage 1 zur Auftragsverarbeitung - Individuelle Vertragsbestandteile**“ weiterzuleiten. Der Auftragnehmer behält sich vor, diese Leistungen nur gegen Entgelt zu erbringen, wie in nach Aufwand (time/material) zu den vereinbarten, und bei Fehlen einer Vereinbarung zu seinen jeweils aktuellen, Sätzen abzurechnen.

5.6 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

5.7 Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen. Gesetzliche Verpflichtungen zur Auskunftserteilung bleiben unberührt.

5.8 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen, einschließlich Inspektionen, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden. Werden solche Prüfungen öfters als ein (1) mal pro Kalenderjahr durch-geführt, ohne dass ein Verstoß des Auftragnehmers gegen diese AVV dazu Anlass gegeben hat, kann der Auftragnehmer Ersatz, der dem Auftragnehmer dadurch entstehenden Aufwände, verlangen.

5.9 Der Auftragnehmer verpflichtet sich, auch die ihm offengelegten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen. Gehen diese Geheimnisschutzregelungen von Art und Umfang her über die Verpflichtungen hinaus, zu deren Einhaltung sich der Auftragnehmer gegenüber dem Auftraggeber gemäß dem Hauptvertrag, insbesondere der AGB des Auftragnehmers, verpflichtet hat, kann der Auftragnehmer Ersatz der dem Auftragnehmer dadurch entstehenden Aufwände verlangen.

5.10 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

5.11 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in

geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Verletzungen des Schutzes personenbezogener Daten nach Art. 33 Abs. 2 DSGVO mit. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lif. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Fernwartung

7.1 Sofern der Auftragnehmer die Pflegeleistungen oder Serviceleistungen auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

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

8. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

8.1 Der Auftragnehmer als Auftragsverarbeiter darf die Auftragsverarbeiter (als Subunternehmer) in Anspruch nehmen, die in der „**Anlage 1 zur Auftragsverarbeitung - Individuelle Vertragsbestandteile**“ genannt sind. Der Einsatz weiterer Auftragsverarbeiter als Subunternehmer muss vom Auftraggeber schriftlich genehmigt werden.

Jedoch darf der Auftragnehmer ohne Genehmigung Auftragsverarbeiter als Subunternehmer einsetzen, wenn diese mit dem Auftragnehmer verbundene Unternehmen i.S.d. §§15ff. AktG sind (allgemeine Genehmigung nach Art. 28 Abs. 2 Satz 1, 2. Alt. DSGVO). In diesem Fall informiert der Auftragnehmer den Auftraggeber über eine solche beabsichtigte Änderung, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Der Auftragnehmer gewährleistet in allen Fällen, dass Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig ausgewählt werden.

8.2 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

8.3 Der Auftragnehmer hat durch geeignete vertragliche Regelungen mit dem Subunternehmer zu vereinbaren, dass die Regelungen der AVV zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten.

8.4 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

8.5 Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

8.6 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

8.7 Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 Satz 2 DSGVO).

9. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

9.1 Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

9.2 Das in „**Anlage 2 zur Auftragsverarbeitung - Technische und organisatorische Maßnahmen**“ beschriebene Datenschutzkonzept (technische und organisatorische Maßnahmen) stellt die Auswahl der technischen und organisatorischen Maßnahmen dar. Diese passen zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer. Unbeschadet bleibt die Verantwortung des Auftraggebers (vgl. Ziffer 1.4).

9.3 Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

9.4 Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Entstehen dem Auftragnehmer dadurch zusätzliche Aufwände, sind diese vom Auftraggeber zu erstatten.

9.5 Die technischen und organisatorischen Maßnahmen kann der Auftragnehmer nach eigenem pflichtgemäßem Ermessen der technischen und organisatorischen Weiterentwicklung anpassen, sie dürfen aber die vereinbarten Standards nicht unterschreiten.

9.6 Der Auftraggeber ist als Verarbeiter von personenbezogenen Daten auf dem ihm überlassenen Speicherplatz in erster Linie selbst verantwortlich, ob und wie er dort personenbezogene Daten verarbeitet. Entsprechend muss der Auftraggeber selbst für „seine“ Datenverarbeitungsvorgänge technische und organisatorische Maßnahmen ergreifen, etwa E-Mails oder Dateien verschlüsseln oder seine Webseiten mit SSL-Zertifikaten versehen, um die Schutzziele aus Art. 32 DSGVO zu erreichen.

10. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

10.1 Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinem Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen.

10.2 Von Ziffer 10.1 unberührt bleibt die Verpflichtung des Auftraggebers aus dem Hauptvertrag, den zum Gebrauch überlassenen Speicherplatz mit Beendigung des Hauptvertrags im gelöschten Zustand an den Auftragnehmer zurückzugeben.

11. Haftung

Auf Art. 82 DSGVO wird verwiesen.

12. Vergütung

12.1 Der Abschluss und die Durchführung der vorliegenden AVV von gripsware ist für den Kunden kostenfrei, sofern das Vertragsmuster des Auftragnehmers unverändert verwendet wird. Sofern der Kunde den Text der AVV verhandeln möchte oder ein eigenes Muster verwenden möchte, kann der Auftragnehmer ein aufwandsbezogenes Entgelt dafür verlangen, insbesondere um höhere Kosten abzudecken. Diese Kosten bzw. anzusetzenden Sätze werden vorab vereinbart. Im Zweifel gelten die in der jeweils aktuellen Preisliste hinterlegten Sätze.

Die Ausfertigung der AVV in elektronischer Form ist kostenfrei, sofern das Vertragsmuster des Auftragnehmers und der unveränderte, online zur Verfügung gestellte Vertragstext (PDF-Dokument) verwendet werden. Will der Auftraggeber ein im Original unterschriebenes Vertragsdokument über den Postverkehr oder per Telefax erhalten, ist der Auftragnehmer berechtigt, dem Auftraggeber eine Aufwandspauschale in Höhe von 10,00 Euro (inkl. der gesetzlichen Umsatzsteuer) zu berechnen.

12.2 Erfolgen Tätigkeiten der Verarbeitung des Auftragnehmers im Datenbestand des Auftraggebers durch technische Zugriffe auf ausdrücklichen Wunsch und nach Weisung des Auftraggebers, so weist der Auftragnehmer den Auftraggeber auf eine eventuelle Kostenpflicht vor Annahme und Durchführung des Auftrags hin und vereinbart die Vergütung hierfür. Im Übrigen sind Leistungen des Kunden-Supports in der Vergütung der Pflegeleistungen gemäß Hauptvertrag inbegriffen.

12.3 Spezielle Weisungen des Auftraggebers im Hinblick auf die Verarbeitung personenbezogener Daten, die über die vertraglich vereinbarten Leistungen und Tarif- bzw. Produktparameter hinausgehen und zu einem Mehraufwand für den Auftragnehmer führen, sind entsprechend gesondert zu vergüten. Insbesondere wenn der Auftragnehmer Tätigkeiten nach

- Ziff. 5.5 - Unterstützung des Auftraggebers bei der Erfüllung der Betroffenenrechte
- Ziff. 5.8 - Häufige Ausübung von Prüfungsrechten
- Ziff. 5.9 - Neue Maßnahmen zum Geheimnisschutz

erbringen soll, kann der Auftragnehmer seine Aufwände (time/material) zu den vereinbarten, und bei Fehlen einer Vereinbarung zu jeweils aktuellen Sätzen, die in der Preisliste auf der Webseite von gripsware unter shop.gripsware.de veröffentlicht sind, abrechnen.

Bei größeren Projekten sollen die Parteien anstreben, einen Einzelauftrag auf Basis der BVB Services abzuschließen.

12.4 Für die Mitwirkung eines Beschäftigten des Auftragnehmers bei Überprüfungen/Inspektionen beim Auftraggeber vor Ort ist der Auftragnehmer berechtigt, dem Auftraggeber die Reise sowie Zeitaufwände gem. den BVB Services und zu jeweils aktuellen Sätzen, die in der Preisliste auf der Webseite von gripsware unter shop.gripsware.de veröffentlicht sind, abzurechnen.

13. Sonstiges

13.1 Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei (3) volle Kalenderjahre aufzubewahren. Längere Aufbewahrungsfristen aufgrund gesetzlicher Bestimmungen bleiben davon unberührt.

13.2 Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

13.3 Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

13.4 Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

13.5 Diese Vereinbarung unterliegt deutschem Recht.

13.6 Ab dem Zeitpunkt des Zustandekommens dieser Vereinbarung werden Verträge über die Auftragsverarbeitung, die in Bezug auf den Hauptvertrag zwischen den Parteien bis zu diesem Zeitpunkt bestehen, durch diese Vereinbarung mit Wirkung für die Zukunft ersetzt.

Anlagen:

- Anlage 1 zur Auftragsverarbeitung - Individuelle Vertragsbestandteile
- Anlage 2 zur Auftragsverarbeitung - Technische und organisatorische Maßnahmen

Anlage 1 zur Auftragsverarbeitung - Individuelle Vertragsbestandteile

1. Vereinbarte Auftragsverarbeitungsleistungen nach Weisung des Auftraggebers:

- Der Gegenstand der Auftragsverarbeitung ergibt sich aus dem Hauptvertrag, der Leistungsbeschreibung und ggfs. dort referenzierten Produkten.
- Der Auftragnehmer bietet standardisierte Produkte im Bereich Bausoftware an und stellt dem Kunden Standard-Baulösungen zur Verfügung. Die Daten sind i.d.R beim Kunden selbst gespeichert. Der Kunde ist als Verarbeiter von personenbezogenen Daten auf dem ihm überlassenen Speicherplatz in erster Linie selbst verantwortlich, ob und wie er dort personenbezogene Daten verarbeitet. Entsprechend muss der Kunde selbst für „seine“ Datenverarbeitungsvorgänge technische und organisatorische Maßnahmen ergreifen, etwa E-Mails verschlüsseln oder seine Webseiten mit SSL- Zertifikaten versehen, um die Schutzziele aus Art. 32 DSGVO zu erreichen.
- Zugriffe des Auftragnehmers auf (ggf. personenbezogene) Daten des Auftraggebers erfolgen ggf. im Rahmen von technischen Hilfestellungen wie z.B. bei Gewährleistungsfällen, Pflegeleistungen oder Serviceleistungen wie Installationsunterstützung, die der Auftraggeber hinsichtlich der auf seine Veranlassung auf den ihm überlassenen Speicherplätzen oder auf eigenen Systemen erzeugten (personenbezogenen) Daten durch Abruf/Weisung beim Auftragnehmer verlangt. Dies betrifft insbesondere Weisungen zur Löschung oder zur Sicherung von Daten.
- Der Auftraggeber behält sich Weisungen im Einzelfall vor, insbesondere im Fall der beim Auftragnehmer angefragten Supportleistungen.

2. Die Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO) im Auftrag des Auftraggebers ist:

- Die Art der Verarbeitung der personenbezogenen Daten wird durch den Auftraggeber bestimmt. Art und Umfang hängen von den durch den Auftraggeber auf seinem Speicherplatz durch ihn installierten Diensten und von der hierzu durch ihn benutzten Software ab.

FTP-Server:

- Auf Wunsch stellt der Auftragnehmer im Rahmen seiner nach dem Hauptvertrag geschuldeten Leistungen dem Auftraggeber Speicherplatz zur Synchronisation seiner Mobilgeräte zur Verfügung. Der Auftraggeber entscheidet selbst, welches der vom Auftragnehmer unterstützten Protokolle (FTP/FTPS/FTPES) genutzt werden soll. Die Daten werden auf dem FTP-Server nur zwischengelagert und nicht verarbeitet. Grundsätzlich sind diese Daten selbst AES256-Bit verschlüsselt.
- Die mit den Hosting-Dienstleistungen verbundenen Verarbeitungsarten betreffen regelmäßig die Speicherung und die Löschung von Daten sowie die Anbindung der Daten an das Internet.

3. Der Zweck der Verarbeitung, der durch den Auftraggeber bestimmt wurde, ist:

- Der Zweck der Verarbeitung von „seinen“, d.h. durch den Auftraggeber auf seinem Speicherplatz verarbeiteten personenbezogenen Daten wird durch den Auftraggeber bestimmt. Je nach den von ihm auf seinen Speicherplätzen installierten Diensten und der hierfür zur Verfügung stehenden Software, wozu auch FTP- und Web-Server-Funktionalitäten gehören, bestimmt der Auftraggeber diese Zwecke allein.
- Die mit den Dienstleistungen durch den Auftraggeber verbundenen Verarbeitungszwecke betreffen die Datenhaltung in Datenbanken.

FTP-Server:

- Der Zweck der Verarbeitung hierbei ist, die Zwischenspeicherung der Daten zu ermöglichen. Diese Zwischenspeicherung dient dem Auftraggeber als eine Art Briefkasten um den Datenaustausch seiner Daten mit seinen Mobilgeräten zu ermöglichen, ohne in seinem Netzwerk eingehende Ports öffnen zu müssen.
- Die vom Mobilgerät des Auftraggebers gesendeten Daten werden kurzzeitig auf dem FTP-Server des Auftragnehmers abgelegt, damit der entsprechende Dienst, der beim Auftraggeber selbst und dauernd läuft, diese Daten abholen kann. Nach dem Abholen werden diese Daten automatisch gelöscht. Ebenso verhält es sich mit Daten, die vom Server des Auftraggebers für das entsprechende Mobilgerät zur Verfügung gestellt werden, diese werden auf dem FTP-Server abgelegt und sobald das Mobilgerät diese Daten abholt, werden auch diese automatisch wieder gelöscht.
- Entsprechende Logfiles (nur FTP-Kommunikation) werden 14-tägig automatisch gelöscht.

Anschrift
Albrecht-Dürer-Str. 2
91334 Hemhofen

Kontakt
Tel. +49 7529 974760
Fax +49 7529 9747669

Bankverbindung
IBAN: DE54 8302 0087 0029 9037 00
BIC: HYVE DE MM 463

Geschäftsführer
Alexander Heilmann
Amtsgericht Fürth HRB 18264

Internet + E-Mail
www.gripsware.de
post@gripsware.de

4. Die Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO), die im Auftrag verarbeitet werden sollen, sind:

- Der Auftraggeber bestimmt mit den von ihm verfolgten Zwecken auch die Art der personenbezogenen Daten, die aufgrund seiner Tätigkeit mit den ihm möglichen Nutzungen auf seinem Speicherplatz verarbeitet werden können.
- Die mit der genutzten Software betroffenen Datenarten betreffen regelmäßig Protokolldateien (Server-Logfiles), Online-Kennungen, E-Mail-Adressen sowie Bestands-, Nutzungs-, und Inhaltsdaten von Benutzern der Auftraggeber-eigenen Webseiten und Datenbanken.

FTP-Server:

- Diese Daten enthalten ausschließlich Daten, die für die Baustellendokumentation notwendig sind (alphanumerische Projektdaten und Mediadaten (Foto, Video, Audio, Skizzen, Dokumente)).
- Dazu gehören auch Projektgrunddaten (Adresse der Baustelle), Adressdaten von beteiligten Personen (z.B. Bauherr, Planer und ausführenden Firmen, inkl. deren Kommunikationsdaten).

5. Die Kategorien der von der Datenverarbeitung betroffenen Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO) sind:

- Der Kunde bestimmt mit den von ihm verfolgten Zwecken auch die Kategorien (Betroffenenkreise) derjenigen natürlichen Personen, deren Daten durch ihn verarbeitet werden.
- Die mit den Hosting-Dienstleistungen betroffenen Personenkategorien sind regelmäßig Webseitennutzer, Datenbankennutzer, FTP-Nutzer und E-Mail-Nutzer.

FTP-Server:

- Auftraggeber und dessen Mitarbeiter (Projekt- und Bauleiter). Die Kunden des Auftraggebers sowie zum Projekt gehörende Planer und ausführende Firmen.

6. Die weisungsberechtigte Person auf Seiten des Auftraggebers ist:

- Der Auftraggeber bzw. der gesetzliche Vertreter des Auftraggebers selbst, oder eine vom Auftraggeber namhaft gemachte und autorisierte Person.

7. Zurzeit tätige Subunternehmer des Auftragnehmers in der Auftragsverarbeitung (Vertragsbetreuung, Support und Rechenzentrum):

- STRATO AG, Pascalstraße 10, 10587 Berlin

8. Weisungsempfänger beim Auftragnehmer:

- Vorname, Name: Der jeweils nach Plan zuständige Mitarbeiter(in) im Kundensupport bzw. in der technischen Abteilung.
- Genaue postalische Adresse: gripsware datentechnik gmbh, Albrecht-Dürer-Str. 2, 91334 Hemhofen
- Telefon (Support): +49 7529 974760
- Telefax (Support): +49 7529 9747669
- E-Mail (Support): support@gripsware.de

9. Kontaktdaten des Ansprechpartners für den Datenschutz:

gripsware datentechnik gmbh
- Datenschutz -
Albrecht-Dürer-Str. 2
91334 Hemhofen
Deutschland

Sobald der Auftragnehmer gemäß § 38 Abs. 1 BDSG und Art. 37 Abs. 1 der DSGVO einen Datenschutzbeauftragten bestellt hat, ist unter dieser Anschrift auch der Datenschutzbeauftragte erreichbar.

Anlage 2 zur Auftragsverarbeitung - Technische und organisatorische Maßnahmen

1. Allgemeines

1.1 Der Auftragnehmer hat unter Berücksichtigung des allgemein üblichen Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die für eine Auftragsverarbeitung erforderlichen technischen und organisatorischen Maßnahmen getroffen, um bei der (Auftrags-)Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die (Auftrags-)Verarbeitung besonderer Kategorien personenbezogener Daten.

1.2 Die nachstehenden entsprechend dem Katalog aus § 64 BDSG (2017) beschriebenen Maßnahmen beziehen sich auf ergriffene Maßnahmen, die im Rahmen der Auftragsverarbeitung erforderlich sind. Aus Sicherheitsgründen erfolgt nachstehend nur eine allgemeine Beschreibung.

1.3 Sämtliche getroffenen Maßnahmen bauen auf der Mitverantwortung des Auftraggebers als „Verantwortlichem“, weil der Auftraggeber vom Auftragnehmer im Rahmen des Hauptvertrags und evtl. zusätzlicher Webhosting-Dienstleistungen einen an das Internet angebundenen Speicherplatz zur Ablage von Informationen/personenbezogenen Daten für Zwecke deren Verarbeitung erhält, der zunächst „leer“ ist. Die Zwecke des „ob“ und des „wie“ der Nutzung bestimmt ausschließlich der Auftraggeber. Entsprechendes gilt für weitere zur Verfügung gestellten sonstigen technischen Dienste. Demzufolge hat der Auftragnehmer zunächst originär keine vertragliche Befugnis, auf diese Daten des Auftraggebers zuzugreifen, selbst wenn dies technisch möglich ist. Die erforderliche Software zur Datenverarbeitung wird durch den Auftraggeber auf seiner eigenen IT installiert und aktiviert. Der Auftragnehmer sorgt lediglich für die technische Einsatzbereitschaft der IT-Systeme entsprechend den vertraglichen Vereinbarungen. Der Auftraggeber ist folglich im Rahmen der durch ihn durchgeführten Datenverarbeitungen der „Herr der Daten“.

1.4 Ausnahmsweise und nur im Rahmen der AVV nimmt der Auftragnehmer Weisungen des Kunden entgegen und verarbeitet nur in diesem Fall personenbezogene Daten des Auftraggebers auf den diesem zur Nutzung überlassenen IT-Systemen in dessen Auftrag und aufgrund dessen Weisung.

Vertraulichkeit

2. Zutrittskontrolle

Gewährleistungsziel: Verwehrung des Zutritts zu Verarbeitungsanlagen, mit denen die (Auftrags-) Verarbeitung durchgeführt wird, für Unbefugte.

Getroffene Maßnahmen:

- Die Geschäftsräume des Auftragnehmers befinden sich in Deutschland.
- Das Webhosting erfolgt ausschließlich auf Datenspeichern, die physikalisch in Deutschland gelegen sind (ausschließlich deutsche Webhoster).
- Beim Auftragnehmer zu den Geschäftsräumen bzw. Hosting-Einrichtungen zutrittsberechtigte Beschäftigte sind organisatorisch festgelegt, Magnetkarten bzw. Schlüssel werden nur entsprechend einer Organisationsanweisung vergeben.

3. Zugangskontrolle

Gewährleistungsziel: Verwehrung des Zugangs zu Datenverarbeitungssystemen, mit denen die (Auftrags-) Verarbeitung durchgeführt wird, für Unbefugte.

Getroffene Maßnahmen:

- Der Zugang zu Datenverarbeitungssystemen ist nur durch Authentifizierung möglich, wenigstens durch ein System von Benutzername und Passwort.
- Im Übrigen sind Zugänge durch ein Berechtigungskonzept (abgestufte Zugriffsberechtigungen) nur besonders autorisierten Beschäftigten vorbehalten.

Anschrift
Albrecht-Dürer-Str. 2
91334 Hemhofen

Kontakt
Tel. +49 7529 974760
Fax +49 7529 9747669

Bankverbindung
IBAN: DE54 8302 0087 0029 9037 00
BIC: HYVE DE MM 463

Geschäftsführer
Alexander Heilmann
Amtsgericht Fürth HRB 18264

Internet + E-Mail
www.gripsware.de
post@gripsware.de

4. Datenträgerkontrolle

Gewährleistungsziel: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

Getroffene Maßnahmen:

- Siehe Ziff. 3
- Soweit auf Weisung des Auftraggebers Daten im Auftrag verarbeitet und personenbezogene Daten auf Festplattenspeicherplätzen als Datenträger gespeichert sind, erfolgen Zugriffe des Auftragnehmers durch ein System von Befugnissen abgestufter Zugriffsberechtigungen durch die Beschäftigten in den Abteilungen Technik (Administration), Support und Buchhaltung. Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch) sind getrennt. Der Zugriff entsprechend Berechtigung wird auch bei Verfahren zur Wiederherstellung von Daten aus Backups gewahrt.
- Es ist Sache des Auftraggebers, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages durch geeignete Techniken (Software) zu verschlüsseln.

5. Speicherkontrolle

Gewährleistungsziel: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Getroffene Maßnahmen:

- Die Bereitstellung der dem Auftraggeber zur Nutzung überlassenen IT-Systeme des Auftragnehmers und die Anbindungen des Auftragnehmers an das Internet erfolgt außerhalb eines Weisungsrechts des Auftraggebers ausschließlich in Verantwortung des Auftragnehmers.
- Der Zugang des Auftraggebers auf die Datenspeicher des Auftragnehmers, mit welchen die Webhosting-Dienstleistungen erbracht werden, erfolgt ausschließlich von außerhalb der Betriebsgebäude des Auftragnehmers über Datenleitungen bzw. das Internet durch ein System der Anmeldung des Auftraggebers mit einem ihm vergebenem Benutzernamen und Passwort.
- Je nach den Nutzungshandlungen, die der Auftraggeber auf dem ihm zur Nutzung überlassenen Datenspeichern vornimmt, ist es alleine seine Verantwortung zu verhindern, dass eine unbefugte Eingabe von personenbezogenen Daten sowie eine unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten erfolgt.
- Soweit jedoch der Auftragnehmer auf Weisung des Auftraggebers tätig wird, um personenbezogene Daten, für die der Auftraggeber „Verantwortlicher“ ist, auf den dem Auftraggeber vom Auftragnehmer bereitgestellten Datenspeichern zu verarbeiten, hat nur ausgewähltes technisches Personal des Auftragnehmers Zugangsrechte auf die betroffenen IT-Systeme.
- Im Übrigen ist es Sache des Auftraggebers, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einer geeigneten Speicherkontrolle zu unterziehen, insbesondere nur geeigneten Dritten (z.B. Webagenturen, Administratoren) Zugang und Zugriff zu gewähren.

6. Benutzerkontrolle

Gewährleistungsziel: Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Getroffene Maßnahmen:

- Soweit im Rahmen der Auftragsverarbeitung durch den Auftragnehmer „Einrichtungen zur Datenübertragung“ in den IT-Systemen des Auftragnehmers genutzt werden, werden diese Einrichtungen durch ein dem allgemein üblichen Stand der Technik entsprechendes Verschlüsselungsverfahren betrieben, wenn der Schutzbedarf eine Verschlüsselung erfordert.
- Sämtliche Beschäftigte des Auftragnehmers, die mit den Daten des Auftraggebers in Berührung kommen könnten, sind zum Personendatenschutz geschult und entsprechend zur Vertraulichkeit verpflichtet.
- Im Übrigen ist es Sache des Auftraggebers, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einer geeigneten Benutzerkontrolle zu unterziehen, insbesondere nur geeigneten Dritten (z.B. Webagenturen, Administratoren) Zugang und Zugriff zu gewähren.

7. Übertragungskontrolle

Gewährleistungsziel: Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Getroffene Maßnahmen:

- Soweit der Auftragnehmer Übermittlungen oder Zurverfügungstellungen auf Weisung des Auftraggebers vornimmt, werden die betroffenen Übermittlungsstellen dokumentiert.
- Soweit erforderlich werden die Daten gegen Zugriffe auf Netzwerkebene geschützt und Schnittstellen gegen unbefugten Datenexport gesichert.
- Im Übrigen ist es Sache des Auftraggebers, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Hauptvertrags einer geeigneten Übertragungskontrolle zu unterziehen, insbesondere nur geeigneten Dritten (z.B. Webagenturen, Administratoren) Zugang und Zugriff zu gewähren und durch eine Verschlüsselung, z.B. SSL/TSL, dafür zu sorgen, dass die von ihm zu übertragenen Daten für Dritte nicht lesbar sind.

8. Zugriffskontrolle

Gewährleistungsziel: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Getroffene Maßnahmen:

- Beim Auftragnehmer hat nur ausgewähltes technisches Personal Zugangsrechte auf die betroffenen IT-Systeme.
- Es ist Sache des Auftraggebers, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einer geeigneten Zugriffskontrolle zu unterziehen, insbesondere nur geeigneten Dritten (z.B. Webagenturen, Administratoren) Zugang und Zugriff zu gewähren.

9. Eingabekontrolle

Gewährleistungsziel: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Getroffene Maßnahmen:

- Es ist Sache des Auftraggebers, ggf. personenbezogene Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einzugeben und dazu, insbesondere nur geeignete Dritte einzusetzen (z.B. Webagenturen, Administratoren). Die Beschäftigten des Auftragnehmers dürfen grundsätzlich nicht auf diese Daten zugreifen bzw. Daten eingeben, verändern oder löschen.
- Das Verarbeiten von personenbezogenen Daten auf den vom Auftragnehmer bereitgestellten Systemen erfolgt somit grundsätzlich durch den Auftraggeber, so dass durch den Auftragnehmer nicht nachträglich überprüft werden und festgestellt werden kann, welche personenbezogenen Daten der Kunde zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert hat.
- Nur im Rahmen seiner Tätigkeiten nach Weisung protokolliert der Auftragnehmer diese Eingaben und Veränderungen in angemessener Weise und dokumentiert die Uhrzeit und den Eingebenden.
- Muss der Auftragnehmer aus gesetzlichen Gründen Informationen entfernen oder den Zugang zu ihnen sperren (etwa im Falle der Nutzung vom Kunden auf den IT-Systemen für Dritte bereit gehaltenen Telemediendiensten bzw. elektronischen Kommunikationsdiensten), wird die Sperrung bzw. die Entfernung von Inhalten protokolliert. Die Protokolldaten werden aufbewahrt und enthalten die Mitarbeiterkennung. Die Löschung erfolgt nach dem Vertragsende automatisiert und wird protokolliert.

10. Transportkontrolle

Gewährleistungsziel: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Getroffene Maßnahmen:

- Die Gewährleistung der Vertraulichkeit der Übermittlung von personenbezogenen Daten wird durch SSL/TSL- Verschlüsselungen über die Webseiten des Auftragnehmers gewährleistet.
- Die Datenträgerentsorgung geschieht durch mechanische vollständige Zerstörung.

— Im Übrigen ist es Sache des Auftraggebers, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einer geeigneten Transportkontrolle zu unterziehen und geeignete Verschlüsselungstechniken einzusetzen.

11. Pseudonymisierung

Gewährleistungsziel: Minimierung der verarbeiteten personenbezogenen Daten, indem Datenfelder, welche die Identifizierung der Betroffenen ermöglichen, so bald wie es bei dem Verarbeitungszweck möglich ist, gelöscht oder transformiert (Anonymisierung, Pseudonymisierung) oder ihre Anzeige in Datenmasken unterdrückt wird, so dass sie den handelnden Personen nicht zur Kenntnis gelangen.

Getroffene Maßnahmen:

— Es ist Sache des Kunden, personenbezogene Daten auf dem ihm überlassenen Speicherplatz selbst zu pseudonymisieren, soweit dies gesetzlich erforderlich ist.

12. Klassifikationsschema für Daten

Getroffene Maßnahmen:

— Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim, vertraulich, intern, öffentlich, normaler Schutzbedarf, durchschnittlicher Schutzbedarf, hoher Schutzbedarf, sensibles Datum).

13. Datenintegrität

Gewährleistungsziel: Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Getroffene Maßnahmen:

— Der Auftragnehmer fertigt Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen und Transaktionshistorien sowie die Dokumentation der Syntax von Daten an.
— Beim Auftragnehmer bestehen Reparaturstrategien und Ausweichprozesse.
— Über die vorstehenden in dieser Ziff. 13 beschriebenen Maßnahmen hinaus, die der Auftragnehmer für seine Daten und Systeme ergreift, ist es Sache des Auftraggebers, für die Datenintegrität des Datenbestandes auf dem ihm überlassenen Speicherplatz selbst Sorge zu tragen.

Verfügbarkeit und Belastbarkeit

14. Verfügbarkeitskontrolle

Gewährleistungsziel: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Getroffene Maßnahmen:

— Der Auftragnehmer hat die Stromversorgung und Netzersatzanlagen auf hohe Ausfallsicherheit ausgelegt.
— Der gesamte Energieverbrauch der Rechenzentren wird über unterbrechungsfreie Stromversorgungen (USV) gewährleistet. Im Falle eines Stromausfalls nehmen die USV-Anlagen eine unterbrechungsfreie Umschaltung mit Shutdown vor. Daneben filtern die USV-Anlagen vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes.

15. Wiederherstellbarkeit

Gewährleistungsziel: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Getroffene Maßnahmen:

— Die eingesetzten Systeme sind technisch redundant vorhanden.
— Der Datenbestand unterliegt einer regelmäßigen Sicherung. Es ist Sache des Auftraggebers, seinen Datenbestand auf dem ihm überlassenen Speicherplatz selbst durch geeignete Sicherungsmaßnahmen vor Datenverlust zu schützen.

16. Trennbarkeit

Gewährleistungsziel: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Getroffene Maßnahmen:

- Beim Auftragnehmer erfolgt eine getrennte Verarbeitung und/oder Lagerung von Daten mit unterschiedlichen Verarbeitungszwecken.
- Beim Auftragnehmer existiert ein System von Befugnissen abgestufter Zugriffsberechtigungen durch die Beschäftigten in den Abteilungen Technik (Administration), Support, Verwaltung und Kundenbuchhaltung.
- Es ist Sache des Auftraggebers, für die Trennung von personenbezogenen Daten auf dem ihm überlassenen Speicherplatz selbst Sorge zu tragen.

17. Zuverlässigkeit

Gewährleistungsziel: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Getroffene Maßnahmen:

- Die Verfügbarkeit der IT-technischen Systeme unterliegt einer regelmäßigen Überwachung.

Auftragsverarbeitung

18. Auftragskontrolle

Gewährleistungsziel: Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Getroffene Maßnahmen:

- Es erfolgt eine Kennzeichnung des Auftragsverarbeitungs-Status gegenüber dem Status der weisungsfreien Datenverarbeitung mit hinterlegtem Auftragsverarbeitungsvertrag und den dazugehörigen Anlagen in der Kundenmaske. Beschäftigte - insbesondere im Rahmen des Telefon-Supports - haben somit ständig Kenntnis über das Vorliegen/Nichtvorliegen eines Auftragsverarbeitungsvertrags.
- Es erfolgt eine Verarbeitung im Auftrag mit standardisierten Vertragsformularen des Auftragnehmers, um eine gleichbleibende Qualität der Auftragsverarbeitung zu gewährleisten. Davon ggf. abweichende Formulare des Auftraggebers werden gegenüber den betroffenen Beschäftigten des Auftragnehmers besonders gekennzeichnet, um Abweichungen in den Standards der Arbeitsabläufe zu erfassen.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

19. Prüfung, Bewertung Evaluierung

Gewährleistungsziel: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung.

Getroffene Maßnahmen:

- Datenschutz-Management
- Regelmäßige Schulung der Beschäftigten des Auftragnehmers
- Der Auftragnehmer setzt einen Kernbestand an langjährig und dauerhaft beschäftigtem Technikerpersonal mit DV-technischer Erfahrung und Expertise ein.