

# Vereinbarung über die Datenverarbeitung im Auftrag

---

nachfolgend „Auftragnehmer“

nachfolgend „Auftraggeber“

gemeinsam nachfolgend „Vertragspartner“

schließen folgende Vereinbarung:

## 1 Gegenstand der Vereinbarung

1.1 Die Vertragspartner haben einen Vertrag über die Nutzung von Software geschlossen (der „Hauptvertrag“). Soweit der Auftragnehmer im Zuge der Erbringung der nach dem Hauptvertrag

Rahmenvertragsnummer:

geschuldeten Leistungen personenbezogene Daten des Auftraggebers verarbeitet, ist der Auftragnehmer Auftragsdatenverarbeiter im Sinne des § 11 BDSG in der bis 25.05.2018 gültigen Fassung bzw. Auftragsverarbeiter im Sinne des Art. 28 DSGVO und § 62 BDSG in der ab 25.05.2018 gültigen Fassung.

1.2 Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG bzw. Art. 44 ff. DSGVO erfüllt sind.

1.3 Aus dem Rahmenvertrag ergeben sich Gegenstand und Dauer des Auftrags, Umfang und Art der Datenverarbeitung sowie der Vertraulichkeit. Zweck der Datenverarbeitung ist die Ermöglichung der Leistungserbringung gemäß dem Rahmen- bzw. Einzelvertrag.

1.4 Art der von der Auftragsdatenverarbeitung betroffenen personenbezogenen Daten:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Mandats- und Verfahrensdaten

1.5 Kategorien betroffener Personen:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten
- Beteiligte an einem Insolvenzverfahren

1.6 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzulegen.

## 2 Rechte und Pflichten des Auftraggebers

2.1 Der Auftraggeber ist für die Beurteilung der Zulässigkeit der Datenverarbeitung und die Wahrung der Rechte der Betroffenen verantwortlich.

- 2.2 Der Auftragnehmer darf personenbezogene Daten des Auftraggebers nur zum Zwecke der Erbringung der Leistungen des Rahmen- bzw. Einzelvertrages und nach Weisung des Auftraggebers verarbeiten. Der Auftraggeber hat ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Verarbeitung personenbezogener Daten.
- 2.3 Weisungen des Auftraggebers
- Weisungen vom Auftraggeber sind schriftlich oder per E-Mail zu erteilen. Alle Weisungen sollen sowohl vom Auftraggeber als auch vom Auftragnehmer zusammen mit dieser Vereinbarung so aufbewahrt werden, dass alle maßgeblichen Regelungen jederzeit verfügbar sind. Der Auftragnehmer ist berechtigt, die Durchführung einer mündlich erteilten Weisung solange auszusetzen, bis sie durch den Auftraggeber schriftlich bestätigt wird.
  - Weisungsberechtigte Personen vom Auftraggeber werden im Laufe der Inbetriebnahme festgelegt und an den Auftragnehmer schriftlich kommuniziert.
  - Weisungsempfänger beim Auftragnehmer werden im Laufe der Inbetriebnahme festgelegt und an den Auftraggeber schriftlich kommuniziert.
  - Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich (E-Mail reicht aus) der Nachfolger oder der Vertreter mitzuteilen. Falls Weisungen die unter Ziff. 1 dieses Auftrags getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt.

### 3 Rechte und Pflichten des Auftragnehmers

- 3.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach den Weisungen des Auftraggebers und für die erforderlichen auftragsbezogenen Tätigkeiten im Rahmen der getroffenen Vereinbarungen. Eine darüberhinausgehende Verarbeitung führt der Auftragnehmer nur dann durch, wenn eine entsprechend Weisung des Auftraggebers vorliegt. Der Auftragnehmer verpflichtet sich, sich nur insoweit Kenntnis von personenbezogenen Daten des Auftraggebers und fremden Geheimnissen zu verschaffen, als dies zur Auftrags Erfüllung erforderlich ist.
- 3.2 Der Auftragnehmer bewahrt das Datenmaterial nicht länger auf, als es der Auftraggeber bestimmt. Gesetzliche Aufbewahrungsfristen bleiben unberührt.
- 3.3 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren. Er bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind.
- 3.4 Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Er verpflichtet sich zur Verschwiegenheit über die vom Auftraggeber überlassenen Daten und Informationen. Der Auftragnehmer ist über die strafrechtlichen Folgen einer Pflichtverletzung belehrt.
- 3.5 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes und der Geheimhaltung vertraut macht und sie auf das Datenschutzgeheimnis und die Vertraulichkeit schriftlich verpflichtet. Der Auftragnehmer überwacht die Einhaltung der datenschutz- und geheimhaltungsrechtlichen Vorschriften.
- 3.6 Der Auftragnehmer wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes und den rechtlichen Vorgaben entsprechendes Datenschutzniveau zu gewährleisten. Die konkreten Maßnahmen sind in Anhang 1 „Technische und organisatorische Schutzmaßnahmen (TOM)“ beschrieben. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftraggeber hat mit Blick auf die Schutzzwecke der für ihn im Auftrag verarbeiteten Daten das Datenschutzkonzept vor Vertragsschluss geprüft und als ausreichend bewertet.
- 3.7 Der Auftragnehmer berichtet, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Rahmen- bzw. Einzelvertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.
- 3.8 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Der Auftragnehmer bestätigt dem Auftraggeber die nach Maßgabe des Rahmen- bzw. Einzelvertrages erfolgte Löschung der Daten. Hiervon ausgenommen sind Daten, für eine gesetzliche oder vertragliche Aufbewahrungsfrist besteht, sowie Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
- 3.9 Unabhängig von sonstigen Regelungen zur Löschung erfolgt die Löschung der Daten in den Sicherungssystemen und -dateien („Backups“) entsprechend dem regulären Turnus der Löschung dieser Backups.
- 3.10 Der Auftragnehmer unterstützt – soweit erforderlich – den Auftraggeber in angemessenem Umfang bei Anfragen und Kontrollen gemäß Ziff. 3.14 und Ziff. 4. Der Auftraggeber hat den Auftragnehmer für seinen Aufwand im Rahmen dieser Unterstützung auf Stundenbasis gemäß der jeweils gültigen Preisliste des Auftragnehmers zu entschädigen.
- 3.11 Der Auftragnehmer wird den Auftraggeber für dessen Datenschutz-Folgenabschätzung angemessen unterstützen.

- 3.12 Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind schriftlich mit dem Auftraggeber abzustimmen.
- 3.13 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- 3.14 Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, wird ihn der Auftragnehmer nach besten Kräften unterstützen.

#### **4 Anfragen Betroffener**

- 4.1 Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson oder einer Behörde verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragnehmer wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.
- 4.2 Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen.

#### **5 Meldung von Störungen und Hinweispflichten des Auftragnehmers**

- 5.1 Der Auftragnehmer überprüft in regelmäßigen Abständen die Einhaltung der Vorgaben dieser Vereinbarung, insbesondere der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Datensicherheit in Anhang 1 zu dieser Vereinbarung. Der Auftragnehmer teilt dem Auftraggeber Störungen bei der Auftrags erledigung und Verletzungen des Datenschutzes, insbesondere der Datensicherheit, mit.
- 5.2 Stellt der Auftragnehmer bei der Prüfung der Ergebnisse Unregelmäßigkeiten oder Fehler fest, informiert er den Auftraggeber hierüber unverzüglich.
- 5.3 Falls der Auftragnehmer der Ansicht ist, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, weist er den Auftraggeber darauf hin. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Der Auftragnehmer ist berechtigt (aber nicht verpflichtet), die Ausführung der Weisung zu unterlassen, bis die Weisung durch den Auftraggeber schriftlich oder per Telefax bestätigt worden ist.

#### **6 Kontrollrechte des Auftraggebers**

- 6.1 Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit nach vorheriger Abstimmung mit dem Auftragnehmer zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufes berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme.
- 6.2 Zur Durchführung der Kontrolle muss der Auftragnehmer nur eine solche Person zulassen, die besonders zur Geheimhaltung, insbesondere in Bezug auf Informationen über den Betrieb des Auftragnehmers, dessen Ausstattung, Geschäftsgeheimnisse des Auftragnehmers und Sicherheitsmaßnahmen, verpflichtet ist. Wird die Kontrolle nicht durch eine dem Auftragnehmer diesbezüglich bereits bekannte Person durchgeführt, muss diese mindestens 7 Werktage vor Durchführung der Kontrolle ihre Legitimation durch den Auftraggeber schriftlich oder per Telefax nachweisen.
- 6.3 Der Auftragnehmer kann für seinen Aufwand im Zusammenhang mit der Kontrolle eine angemessene Vergütung verlangen.
- 6.4 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn der Auftraggeber bei solchen Prüfungen oder in sonstiger Weise Fehler oder Unregelmäßigkeiten feststellt.
- 6.5 Sonstige vertragliche oder gesetzliche Kontrollrechte des Auftraggebers bleiben unberührt.

#### **7 Einsatz von Subunternehmen**

- 7.1 Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in dem Anhang 2 aufgeführten Unternehmen als Subunternehmer für Teilleistungen für den Auftragnehmer tätig und können in diesem Zusammenhang auch Zugriff auf die personenbezogenen Daten des Auftraggebers haben. Für diese Subunternehmer gilt die Einwilligung für das Tätigwerden als erteilt.
- 7.2 Die Beauftragung von Subunternehmen nach Vertragsabschluss durch den Auftragnehmer ist durch den Auftraggeber zustimmungspflichtig. Der Auftragnehmer stellt beim Auftraggeber in Schriftform eine Anfrage zur Freigabe des Subunternehmens. Sollte sich der Auftraggeber nicht innerhalb von 2 Wochen in Schriftform zu der Freigabe äußern oder der Zustimmung aus einem wichtigen Grund widersprechen, so gilt die Zustimmung zum Subunternehmen als erteilt.
- 7.3 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Der Auftragnehmer verpflichtet sich, die eingeschalteten Subunternehmen in Textform zur Verschwiegenheit und Vertraulichkeit hinsichtlich der

vom Auftraggeber überlassenen Geheimnisse zu verpflichten. Eine etwaige Prüfung durch den Auftraggeber beim Subunternehmer erfolgt nur in Abstimmung mit dem Auftragnehmer. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

- 7.4 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen, IT-Hosting oder Wartung. Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

## 8 Datenschutzbeauftragter

- 8.1 Der Auftragnehmer sichert zu, dass er, soweit erforderlich, entsprechend den gesetzlichen Bestimmungen bei der zuständigen Aufsichtsbehörde gemeldet ist und einen betrieblichen Datenschutzbeauftragten entsprechend den gesetzlichen Vorgaben ausgewählt und bestellt hat. Der betriebliche Datenschutzbeauftragte des Auftragnehmers nimmt seine Aufgaben nach den einschlägigen gesetzlichen Bestimmungen wahr.

## 9 Laufzeit und Kündigung

- 9.1 Diese Vereinbarung richtet sich nach den Laufzeiten und Kündigungsfristen des Rahmenvertrags zwischen den Parteien.
- 9.2 Mit Beendigung des Rahmenvertrags endet diese Vereinbarung automatisch, ohne dass es einer gesonderten Kündigung bedarf. Endet der Rahmenvertrag während darunter abgeschlossene Einzelverträge noch nicht vollständig erfüllt sind, so endet diese Vereinbarung automatisch erst mit der vollständigen Erfüllung des letzten unter dem Rahmenvertrag abgeschlossenen Einzelvertrages. Die Pflichten aus dieser Vereinbarung über die Auftragsdatenverarbeitung gelten in jedem Fall auch nach einer Beendigung des Rahmenvertrags bis zur vollständigen Vernichtung oder Rückgabe aller im Zusammenhang mit dem Rahmenvertrag stehenden Daten durch den Auftragnehmer.
- 9.3 Mit der Beendigung dieser Vereinbarung gemäß dieser Ziffer 9 endet die Tätigkeit des Auftragnehmers für den Auftraggeber.

## 10 Schlussbestimmungen

- 10.1 Wird eine vom Auftragnehmer im Zusammenhang mit der Bereitstellung des Dienstes geschuldete Leistung aufgrund einer Weisung vom Auftraggeber unmöglich gemacht oder wesentlich erschwert oder verlangt der Auftraggeber eine Löschung von Daten vor Ende des Auftrags, und ist der Auftragnehmer aufgrund der Löschung ganz oder teilweise an der weiteren Leistungserbringung gehindert, so wird der Auftragnehmer insoweit von seinen Leistungspflichten frei. Der Anspruch des Auftragnehmers auf die vereinbarte Vergütung bleibt hiervon unberührt.
- 10.2 Erhöht sich aufgrund einer Weisung vom Auftraggeber für den Auftragnehmer der für die Leistungserbringung erforderliche Aufwand, kann der Auftragnehmer eine entsprechende Anpassung der vereinbarten Vergütung verlangen. Der Auftragnehmer hat den Auftraggeber vor der zusätzlichen Leistungserbringung auf die zusätzlichen Kosten hinzuweisen und der Auftraggeber hat die Möglichkeit die Weisung zurückzunehmen, sodass keine zusätzlichen Kosten entstehen.
- 10.3 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »verantwortlicher Stelle« im Sinne des BDSG bzw. der DSGVO liegen.
- 10.4 Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Rahmen- bzw. Einzelvertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
- 10.5 Es gilt deutsches Recht.
- 10.6 Die Anhänge sind Bestandteil dieses Vertrages:
- Anhang 1 Technische und organisatorische Schutzmaßnahmen
  - Anhang 2 Zugelassene Subunternehmer

Ort, Datum



Unterschrift STP Informationstechnologie AG

Ort, Datum

Unterschrift Auftraggeber

## Anhang 1 zur Vereinbarung über die Auftragsdatenverarbeitung

### Technische und organisatorische Schutzmaßnahmen (TOM)

Der Auftragnehmer trifft Maßnahmen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind zur:

#### 1 Zutrittskontrolle

- 1.1 Zutrittskontrolle, also Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
- 1.2 Maßnahmen:
  - a) Der Zugang zu den Räumlichkeiten des Auftragnehmers ohne besondere Aufsicht ist ausschließlich registrierten KeyCard-Besitzern gewährt.
  - b) Der Zugang zum Serverraum ist nur der Geschäftsführung und den Administratoren gewährt.
  - c) Sämtliche Zugangstüren der Räumlichkeiten des Auftragnehmers sind mit Keycardsystem ausgestattet. Die Keycardausgabe wird mit Anzahl und Art der Keycard, Name des Mitarbeiters, Datum sowie Unterschrift des Mitarbeiters durch die Personalabteilung dokumentiert.
  - d) Der Zutritt zu den Räumlichkeiten des Auftragnehmers für firmenfremde Personen ist nur unter Aufsicht durch einen Mitarbeiter des Auftragnehmers in den Räumlichkeiten des Auftragnehmers zugelassen.

#### 2 Zugangskontrolle

- 2.1 Zugangskontrolle, also zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
- 2.2 Maßnahmen:
  - a) Nutzerkennungen an Workstations, Laptops, Servern etc., d.h. Nutzernamen und Passwörter sind an den jeweiligen Nutzer gebunden und dürfen nicht weitergegeben werden.

#### 3 Zugriffskontrolle

- 3.1 Zugriffskontrolle, also zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen 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.
- 3.2 Maßnahmen:
  - a) Diese Maßnahme ist eng an die Zugangskontrolle gebunden. Berechtigte Personen, die sich mit ihrer Nutzerkennung ordnungsgemäß am DV-System identifiziert haben, besitzen entsprechend ihrer Nutzerrechte differenzierte und damit abgestufte Berechtigungen in den jeweiligen Software-Systemen. Regelmäßig erfolgt dies entsprechend eines Rollen- und Rechtekonzeptes.
  - b) Der administrative Zugriff auf zentrale DV-Systeme wie bspw. Server oder Netzwerk ist den IT-Administratoren vorbehalten.

#### 4 Weitergabekontrolle

- 4.1 Weitergabekontrolle, also zu 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.
- 4.2 Maßnahmen:
  - a) Wege der Datenübertragung sind grundsätzlich vorab mit dem Auftraggeber abzustimmen.
  - b) Soweit eine Speicherung von personenbezogenen Daten vor Ort auf ein mobiles Speichermedium zum Transport erfolgt, werden die Daten verschlüsselt und der Auftragnehmer wird angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen.
  - c) Der Auftragnehmer wird die, auf seinem Datenverarbeitungssystem und mobilen Speichermedien gespeicherten Daten nach Beendigung der Tätigkeit löschen. Die Datenlöschung wird vom Auftragnehmer dokumentiert.

#### 5 Eingabekontrolle

- 5.1 Eingabekontrolle, also zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
- 5.2 Maßnahmen:
  - a) Es findet beim Auftragnehmer keine generelle Protokollierung der einzelnen Arbeitsschritte statt.
  - b) Ein diesbezügliches Erfordernis ist dem Auftragnehmer vor Auftragsdurchführung durch den Auftraggeber schriftlich mitzuteilen.

## 6 Auftragskontrolle

- 6.1 Auftragskontrolle, also zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
- 6.2 Maßnahmen:
- Zwischen Auftragnehmer und einem etwaigen Subunternehmer gibt es entsprechende Vereinbarungen die zumindest dem Sicherheitsniveau der Vereinbarungen zwischen Auftraggeber und Auftragnehmer entsprechen.
  - Sämtliche Mitarbeiter wurden zur Wahrung des Datengeheimnisses verpflichtet.

## 7 Verfügbarkeitskontrolle

- 7.1 Verfügbarkeitskontrolle, also zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
- 7.2 Maßnahmen:
- Alle Rechner sind mit einem aktuellen Virenschutz ausgestattet. Das interne Netzwerk ist per Firewall vor externem Zugriff geschützt. Sofern erforderlich wird täglich ein komplettes Backup der Daten durchgeführt, sofern dies nicht systemseitig lediglich durch den Auftraggeber erfüllt werden kann. Die Daten werden nach Beendigung des Auftrages gelöscht.

## 8 Trennungsgebot

- 8.1 Trennungsgebot, also zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
- 8.2 Maßnahmen:
- Daten separater Aufträge werden grundsätzlich unabhängig voneinander verarbeitet und nicht zusammengeführt.
  - Daten des Auftraggebers werden getrennt von Fremddaten abgelegt.

## Anhang 2 zur Vereinbarung über die Auftragsdatenverarbeitung

### Zugelassene Subunternehmer sind:

1	STP Holding GmbH	Dienstleister	Lorenzstraße 29 76135 Karlsruhe Deutschland
2	STP Portal GmbH	Technologie	Lorenzstraße 29 76135 Karlsruhe Deutschland