Datenschutz- und Datensicherheitsbestimmungen, Stand 01/2019

zwischen dem Vertragsnehmer (nachstehend AUTRAGGEBER genannt) und VR Payment GmbH, Saonestraße 3a, 60528 Frankfurt am Main (nachstehend AUFTRAGNEHMER genannt).

1. Die vorliegende Anlage „Datenschutz – und Datensicherheitsbestimmungen" (DuD-B) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Vertrag ergeben. Sie findet Anwendung auf alle Leistungen oder Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Mitarbeiter des AUFTRAGNEHMERS oder durch den AUFTRAGNEHMER mit schriftlicher Zustimmung des AUFTRAGGEBERS beauftragte Subunternehmer personenbezogenen Daten des AUFTRAGGEBERS verarbeiten.
2. Die Haftung der Parteien untereinander für Schäden im Zusammenhang mit der Auftragsverarbeitung richtet sich nach den Bestimmungen der DuD-B. Enthält die DuD-B keine diesbezüglichen Regelungen, gelten die gesetzlichen Bestimmungen (insbesondere Art. 82 Abs. 5 DS-GVO).
3. Die DuD-B finden weiterhin Anwendung bei Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen (Prüfung, Wartung und Pflege von Hard- oder Software), wenn dabei eine Verarbeitung, insbesondere der Zugriff auf personenbezogene Daten, nicht ausgeschlossen werden kann.

Die DuD-B bestehen aus:

Teil 1: Konkrete Angaben zur Auftragsverarbeitung
Teil 2: Allgemeine Regelungen zur Auftragsverarbeitung
Teil 3: Vereinbarung zur Festlegung der technischen und organisatorischen Maßnahmen

Teil 1

Konkrete Angaben zur Auftragsverarbeitung

Gemäß Art. 28 Abs. 3 Datenschutz–Grundverordnung (DS-GVO) sind folgende konkrete Angaben für den Auftrag festzulegen, sofern sie nicht bereits im Vertrag einschließlich seiner Anlagen geregelt wurden:

1. Gegenstand des Auftrages

Der AUFTRAGNEHMER verarbeitet personenbezogene Daten im Auftrag des AUFTRAGGEBERS.
Der Gegenstand des Auftrags ergibt sich im Einzelnen aus dem schriftlichen Vertrag, auf den hier verwiesen wird. Soweit im Vertrag auf die Aufgaben des AUFTRAGNEHMERS Bezug genommen wird, sind die jeweiligen Vertragsvorschriften wesentlicher Bestandteil dieses Auftrages.

2. Dauer des Auftrages

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Vertrags.

3. Verarbeitung von Daten

a) Zweck der Verarbeitung
Hosting der Anwendung VR pay QuickCommerce.

b) Art der Verarbeitung (Beschreibung der einzelnen Verarbeitungsschritte)
Zur Erfüllung seiner Aufgaben und Erbringung seiner Leistungen gemäß vorliegendem Auftrag führt der Auftragnehmer die folgenden Arbeitsschritte durch:
Der AUFTRAGNEHMER wird die vom AUFTRAGGEBER zur Verfügung gestellten Daten (vgl. nachfolgende Ziffer 4 „Art der Daten") in seinen Systemen verarbeiten. Die Daten werden zur Anlage eines Benutzerkontos sowie zur Auftrags- und Zahlungsabwicklung verwendet. Die Daten können im Rahmen einer Hotline- oder Servicetätigkeit eingesehen werden.

4. Art der Daten

Im Zusammenhang mit der vorbeschriebenen Leistungserbringung werden vom AUFTRAGNEHMER folgende Datenarten/-kategorien verarbeitet:

- Personenstammdaten (wie z.B. Vor- und Nachname, Geburtsdatum)
- Kommunikationsdaten (wie z.B. Telefon, E-Mail-Adresse)
- Adressdaten (wie z.B. Straße, Ort)
- Zahlungsdaten
- Vertragsstammdaten (wie z.B. Vertragsbeziehung, Produktinteresse)
- Nutzerverhalten

5. Kategorien der betroffenen Personen

Die Kategorien der Personen, die durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags betroffen sind, umfassen Kunden, Interessenten oder Abonnenten des Vertragspartners sowie Mitarbeiter und Lieferanten des Auftraggebers.

6. Umfang der Weisungsbefugnisse, Verantwortliche Ansprechpartner bei den Parteien

Der AUFTRAGNEHMER darf während der Dauer des Auftrages die personenbezogenen Daten ausschließlich für die Zwecke gemäß Ziffer 1 entsprechend den unter Ziffer 3 Buchstabe b) dargestellten Verarbeitungsschritten verarbeiten, wenn und soweit dies mit den Bestimmungen zum Schutz personenbezogener Daten vereinbar ist. Darüber hinaus hat der AUFTRAGNEHMER alle weiteren konkreten und/oder generellen schriftlichen Weisungen des AUFTRAGGEBERS über Art, Umfang und Verfahren der Datenverarbeitung nach Maßgabe dieser DuD-B zu befolgen.
Weisungsberechtigte Personen des AUFTRAGGEBERS ist die als Vertragspartner genannte Person.
Weisungsempfänger beim Auftragnehmer sind beim Auftragnehmer tätige Mitarbeiter, die im Zusammenhang mit VR pay QuickCommerce in ihrem Aufgabenbereich für die Auftragsabwicklung zuständig sind und die berechtigterweise Zugriff auf die personenbezogenen Daten haben.

Betrieblicher Datenschutzbeauftragter des AUFTRAGGEBERS kann dem Impressum der öffentlichen Webseiten des Vertragspartners entnommen werden.
Betrieblicher Datenschutzbeauftragter des AUFTRAGNEHMERS ist: datenschutz@vr-payment.de
Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners oder des Datenschutzbeauftragten ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. Vertreter mitzuteilen.

7. Etwaige Zustimmung zur Beauftragung von Subunternehmern

Der AUFTRAGNEHMER darf folgenden/folgende Subunternehmer einsetzen:
- Payrexx AG
- Payreto GmbH

Der/die vorgenannte/n Subunternehmer wird/werden mit folgenden Leistungen beauftragt:
- Betrieb der Plattform VR pay QuickCommerce
- Durchführung von Hotline- und Servicedienstleistungen.

8. Geltung der Anlage „Datenschutz- und Datensicherheitsbestimmungen“ (DuD-B)

Die DuD-B ist wesentlicher Bestandteil des Vertrages zwischen den Parteien.

Teil 2

Allgemeine Regelungen zur Auftragsverarbeitung

§ 1 Allgemeine Bestimmungen

1. Der AUFTRAGGEBER ist als „Verantwortlicher" i.S.d. Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) für die Einhaltung der Vorschriften über den Datenschutz, für die Rechtmäßigkeit der Datenverarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO, insbesondere der Datenweitergabe an den AUFTRAGNEHMER, sowie für die Wahrnehmung der Rechte der Betroffenen verantwortlich. Der AUFTRAGNEHMER hat den AUFTRAGGEBER hierbei in geeigneter Weise zu unterstützen. Darüber hinaus verpflichtet sich der AUFTRAGNEHMER zur Einhaltung sämtlicher einschlägiger datenschutzrechtlicher Vorschriften im Rahmen der Ausführung des Auftrages.
2. Sofern der AUFTRAGGEBER im Rahmen des jeweiligen Auftrages seinerseits selbst Dienstleister anderer Auftraggeber ist, stehen die Rechte aus dieser Anlage auch diesen anderen Auftraggebern zu.
3. Bei der E-Mail-Kommunikation werden die Parteien die Vertraulichkeit beachten, indem sie vertrauliche Informationen gegen unberechtigte Kenntnisnahme oder Manipulationen schützen. Hierzu können die Parteien entsprechende technische Maßnahmen, z.B. Verschlüsselungs- und Signaturverfahren, abstimmen.
4. Dem AUFTRAGNEHMER ist bekannt, dass ein Verstoß gegen datenschutzrechtliche Vorschriften eine Ordnungswidrigkeit und gegebenenfalls auch eine Straftat darstellen kann.
5. Der AUFTRAGNEHMER bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind und dass der AUFTRAGGEBER und der AUFTRAGNEHMER und gegebenenfalls deren Vertreter bei Anfragen der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten.
6. Der AUFTRAGNEHMER bestätigt und stellt sicher, dass die für die Durchführung des Auftrags eingesetzten Personen zur Vertraulichkeit schriftlich verpflichtet sind und in die Schutzbestimmungen der DS-GVO eingewiesen worden sind. Die gleiche Verpflichtung gilt für weitere Bestimmungen zum Datenschutz (z.B. § 88 TKG sowie §§ 203, 206 StGB), sofern diese im konkreten Auftrag einschlägig sind. Auf Verlangen des AUFTRAGGEBERS wird der AUFTRAGNEHMER die Verpflichtung und Einweisung nachweisen.
7. Der AUFTRAGNEHEMER muss geeignete, wirksame und dokumentierte Maßnahmen implementieren, welche die Einhaltung der datenschutzrechtlichen Vorgaben sicherstellen, insbesondere im Hinblick auf das Erkennen und rechtzeitige Melden von Datenschutzverstößen.
8. Soweit der AUFTRAGNEHMER seine Leistung in den Räumlichkeiten oder unter Zugriff auf die Systeme des AUFTRAGGEBERS erbringt, unterliegt er den Kontrolleinrichtungen des AUFTRAGGEBERS (insbesondere Zutritts-, Zugangs- und Zugriffskontrolle).
9. Der AUFTRAGNEHMER ist für die Durchführung des Auftrages verpflichtet, nach Maßgabe der geltenden datenschutzrechtlichen Vorschriften einen Beauftragten für den Datenschutz schriftlich zu bestellen. Der AUFTRAGNEHMER wird dem AUFTRAGGEBER den Namen des Beauftragten für den Datenschutz benennen. Bei einem Wechsel des Beauftragten für den Datenschutz wird der AUFTRAGNEHMER den AUFTRAGGEBER unverzüglich hiervon in Kenntnis setzen. Soweit der AUFTRAGNEHMER nach Maßgabe der geltenden datenschutzrechtlichen Vorschriften nicht zur Bestellung eines Beauftragten für den Datenschutz verpflichtet ist, stellt er die Erfüllung der Aufgaben nach den geltenden datenschutzrechtlichen Vorschriften in anderer geeigneter Weise sicher. Der AUFTRAGNEHMER kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
10. Der AUFTRAGNEHMER kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
11. Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER bei der Einhaltung der DS-GVO zur Sicherheit personenbezogener Daten, bei Meldepflichten bei Datenpannen, ggf. bei einer Datenschutz-Folgeabschätzungen und vorherige Konsultationen und insbesondere zur Erfüllung der Rechte der betroffenen Person gemäß Art.12 – 23 DS-GVO.
12. Datenschutzrechtliche Auskünfte an Betroffene oder durch Sie beauftragte Dritte darf der AUFTRAGNEHMER nur nach vorheriger schriftlicher Zustimmung durch den AUFTRAGGEBER erteilen.
13. Der AUFTRAGNEHMER und gegebenenfalls sein Vertreter und Subunternehmer führen ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu allen Kategorien von im Auftrag des AUFTRAGGEBERS durchgeführten Tätigkeiten der Verarbeitung. Der AUFTRAGNEHMER wird dem AUFTRAGGEBER auf Anforderung die für diesen Vertrag relevanten Inhalte aus seinem Verarbeitungsverzeichnis zur Verfügung stellen.
14. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB des AUFTRAGNEHMERS gegenüber dem AUFTRAGGEBER ist hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

15. Änderungen, Ergänzungen und Nebenabreden sowie einseitig abzugebende Willenserklärungen, wie z.B. Weisungen, Bestätigungen oder Zustimmungen, bedürfen der Schriftform gem. § 126 Bürgerliches Gesetzbuch (BGB). Dies gilt auch für Änderungen der Schriftformklausel.
16. Der AUFTRAGNEHMER verarbeitet personenbezogene Daten im Auftrag des AUFTRAGGEBERS. Dies umfasst Tätigkeiten, die im Hauptvertrag und in dieser Anlage konkretisiert sind.

§ 2 Ort der Datenverarbeitung

1. Die Verarbeitung der Daten erfolgt ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union, der Schweiz oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Falls die Anwendung der DS-GVO in den Staaten des EWR nicht verbindlich beschlossen wurde, gelten die Staaten des EWR als Drittländer.
2. Die Datenverarbeitung in Drittländern ist ohne Zustimmung des Auftraggebers unzulässig. Dies gilt auch für Subunternehmer, wobei darauf hingewiesen wird, dass unter „Verarbeitung" auch die Möglichkeit der Einsichtnahme, etwa im Rahmen von Fernwartungszugriffen zu verstehen ist. Wartungsarbeiten von Subunternehmern in Drittländern sind über Datenschutzverträge abzusichern.
3. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des AUFTRAGGEBERS und kann nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.
4. Die Verarbeitung von Daten außerhalb von Betriebsstätten des AUFTRAGNEHMERS (z.B. Heim-/Telearbeit, Remotezugriff) ist zulässig. Heim-/Telearbeit ist durch Zusatzvereinbarungen sicherheits- und datenschutztechnisch abzusichern. Der Datenschutzbeauftragte des Auftragsnehmers führt hierzu entsprechende Kontrollmechanismen nachweisbar ein.

§ 3 Weisungsrecht und Zweckbindung

1. Bei der Verarbeitung personenbezogener Daten wird der AUFTRAGNEHMER für den AUFTRAGGEBER tätig und ist insoweit verpflichtet, die Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und für Zwecke des AUFTRAGGEBERS zu verarbeiten und dabei den schriftlichen Weisungen des AUFTRAGGEBERS zu folgen.
2. Kopien oder Duplikate werden ohne Wissen des AUFTRAGGEBERS nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
3. Mündliche Weisungen sind unverzüglich schriftlich durch den AUFTRAGNEHMER zu bestätigen. Die schriftliche Bestätigung der mündlichen Weisungen muss von AUFTRAGGEBER und AUFTRAGNEHMER so aufbewahrt werden, dass alle maßgeblichen Regelungen jederzeit verfügbar sind.
4. Der AUFTRAGNEHMER hat den AUFTRAGGEBER unverzüglich darauf aufmerksam zu machen, wenn eine vom AUFTRAGGEBER erteilte Weisung seiner Meinung nach gegen Vorschriften über den Datenschutz verstößt.

§ 4 Unverzüglich Meldungen und Informationspflichten bei Datenschutzverletzungen

1. Der AUFTRAGNEHMER hat den AUFTRAGGEBER bei Unregelmäßigkeiten des Datenverarbeitungsablaufes, bei begründetem Verdacht der Verletzung von Vorschriften und vertraglichen Vereinbarungen zum Schutz personenbezogener Daten, Verstöße des AUFTRAGNEHMERS oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen, sowie bei Beanstandungen durch eine Datenschutzaufsichtsbehörde, eine Revision oder in sonstigen Datenschutzprüfungsberichten, sofern ihm dies nicht aufgrund einer behördlichen Vorgabe im Rahmen eines Ermittlungsverfahrens untersagt ist, zu informieren und die Abhilfemaßnahmen aufzuzeigen (Datenschutzverletzung). Der AUFTRAGNEHMER sichert zu, den AUFTRAGGEBER bei möglichen Informationspflichten nach Artikel 33 – 34 DS-GVO zu unterstützen.
2. Die Meldung an den AUFTRAGGEBER muss unverzüglich und möglichst binnen 24 Stunden, nachdem dem AUFTRAGNEHMER die Verletzung bekannt wurde erfolgen.
3. Jede Datenschutzverletzung ist vom AUFTRAGNEHMER zu dokumentieren. Die Dokumentation und Meldung einer Datenschutzverletzung enthält mindestens folgende Informationen:
   - 3.1 eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
   - 3.2 den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
   - 3.3 eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3.4 eine Beschreibung der von dem AUFTRAGNEHMER ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Darüber hinaus hat der AUFTRAGNEHMER dem AUFTRAGGEBER alle sonstigen Informationen zu erteilen, die der AUFTRAGGEBER für die Erfüllung seiner eigenen Meldepflichten benötigt.

4. Sofern die Möglichkeit besteht, dass das Eigentum des AUFTRAGGEBERS an den Daten beim AUFTRAGNEHMER durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet wird oder absehbar gefährdet werden könnte, so hat der AUFTRAGNEHMER den AUFTRAGGEBER unverzüglich zu verständigen.
5. Der AUFTRAGNEHMER hat dem AUFTRAGGEBER alle aus einer Datenschutzverletzung entstehenden Schäden, insbesondere die Kosten für die Benachrichtigung der Betroffenen oder ein etwaiges Bußgeld bei Verletzung der Selbstanzeigepflicht nach Artikel 33 – 34 DS-GVO zu ersetzen, sofern dem ein schuldhaftes Verhalten des AUFTRAGNEHMERS zugrunde liegt.

§ 5 Subunternehmer

1. Der Einsatz von Subunternehmern durch den AUFTRAGNEHMER und/oder weiterer Subunternehmer (Kettenbeauftragung) bedarf der vorherigen schriftlichen Zustimmung des AUFTRAGGEBERS.
2. Der AUFTRAGGEBER behält sich vor, die Zustimmung lediglich zu erteilen, nachdem der AUFTRAGNEHMER Namen und Anschrift des Subunternehmers mitgeteilt hat. Ferner behält sich der AUFTRAGGEBER vor, die Zustimmung lediglich zu erteilen, sofern vom AUFTRAGNEHMER nachgewiesen wurde, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat.
3. Der AUFTRAGNEHMER hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen AUFTRAGGEBER und AUFTRAGNEHMER auch gegenüber Subunternehmern gelten. Insbesondere muss der AUFTRAGGEBER berechtigt sein, Kontrollen vor Ort beim Subunternehmer durchzuführen oder durch Dritte durchführen zu lassen. Der AUFTRAGNEHMER hat die Einhaltung der Pflichten regelmäßig zu überprüfen.
4. Die schriftlich zu treffenden, vertraglichen Vereinbarungen zwischen dem AUFTRAGNEHMER und dem Subunternehmer sind so zu gestalten, dass sie den Regelungen der vorliegenden Anlage entsprechen. Zu diesem Zweck müssen insbesondere die mit dem Subunternehmer zu vereinbarenden technischen und organisatorischen Maßnahmen ein gleichwertiges Schutzniveau aufweisen; die Weisungs- und Kontrollrechte müssen uneingeschränkt erhalten bleiben und die Datenverarbeitung muss weiterhin in der EU/EWR erfolgen.
5. Auf Anforderung des AUFTRAGGEBERS wird der AUFTRAGNEHMER Auskunft über den wesentlichen Vertragsinhalt mit dem Subunternehmer und die Umsetzung der datenschutzrelevanten Verpflichtungen geben, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen.
6. Bedient sich der AUFTRAGNEHMER bei der Erbringung der Leistung gegenüber dem AUFTRAGGEBER eines Subunternehmers, wird der AUFTRAGNEHMER dem AUFTRAGGEBER unverzüglich auf Verlangen die Dokumentation und das Ergebnis der vom AUFTRAGNEHMER in Bezug auf den Subunternehmer durchgeführten Erstkontrolle und regelmäßigen Kontrollen bzw. die Einhaltungsbestätigungen des Subunternehmers zugänglich machen.
7. Der AUFTRAGNEHMER bleibt für die Erfüllung der auf den Subunternehmer übertragenen Tätigkeiten im gleichen Umfang verantwortlich, als würden diese durch den AUFTRAGNEHMER selbst ausgeführt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

§ 6 Berichtigung, Einschränkung, Löschung und Rückgabe von Daten

1. Der AUFTRAGNEHMER darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des AUFTRAGGEBERS berichtigen, löschen oder deren Verarbeitung einschränken. Gibt der Auftraggeber keine konkreten Fristen vor, gelten die gesetzlichen Aufbewahrungs- und Löschfristen.
2. Der AUFTRAGGEBER kann vorbehaltlich gesetzlicher Aufbewahrungspflichten oder sonstiger entgegenstehender Rechtsvorschriften auch während der Laufzeit und nach Beendigung des Vertrages jederzeit die Berichtigung, Löschung, Sperrung (i.S.d. Einschränkung der Verarbeitung gem. Art. 4 Nr. 3 DS-GVO) und Herausgabe von personenbezogenen Daten verlangen.
3. Nach Abschluss der vertraglichen Arbeiten hat der AUFTRAGNEHMER, sämtliche in seinen Besitz gelangten Unterlagen, wie z.B. Test- und Ausschussmaterial, Datensicherungskopien und erstellten Verarbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzkonform zu löschen oder dem AUFTRAGGEBER auszuhändigen. Dokumente, Daten und Kopien die nicht ausgehändigt werden können sind nach Abschluss der vertraglichen Arbeiten zu löschen. Die Löschung ist durch ein entsprechendes Löschprotokoll nachzuweisen. Gesetzliche Aufbewahrungspflichten, denen der AUFTRAGNEHMER unterliegt insbesondere nach Abgabenordnung und

HGB, bleiben hiervon unberührt. Vertragsbezogene Daten (z.B. Ansprechpartner des AUFTRAGGEBERS), die zur Sicherung von Beweisinteressen des AUFTRAGNEHMERS erforderlich sind, dürfen in gesperrter Form bis zum Ablauf der hierfür geltenden Verjährungsfrist aufbewahrt werden. Die Löschung ist dem AUFTRAGGEBER auf Anforderung schriftlich zu bestätigen. Zurückbehaltungsrechte des AUFTRAGNEHMERS sind ausgeschlossen.

4. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den AUFTRAGNEHMER wendet, wird der AUFTRAGNEHMER dieses Ersuchen unverzüglich an den AUFTRAGGEBER weiterleiten.

§ 7 Technische und organisatorische Sicherheitsmaßnahmen nach Art.32 DS-GVO

1. Der AUFTRAGNEHMER wird seine Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.
2. Der AUFTRAGNEHMER hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem AUFTRAGGEBER zur Prüfung zu übergeben.
3. Der AUFTRAGNEHMER beachtet die Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1, Abs. 2 DS-GVO und gewährleistet die vertraglich vereinbarten und gesetzlich erforderlichen Datensicherheitsmaßnahmen gem. Art. 24, Art. 28, Art. 32 DS-GVO, um den Nachweis zu erbringen, dass die Verarbeitung gemäß der DS-GVO erfolgt.
4. Der AUFTRAGNEHMER darf Zugriffsberechtigungen nur an Personen vergeben, die mit der Durchführung des Auftrags befasst sind. Die Berechtigungen sind nur in dem für die Erfüllung der jeweiligen Aufgaben erforderlichen Umfang zu vergeben. Auf Verlangen wird der AUFTRAGNEHMER dem AUFTRAGGEBER die zugriffsberechtigten Personen und deren Berechtigungen benennen.
5. Der AUFTRAGNEHMER sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
6. Der AUFTRAGNEHMER ist nicht befugt, ohne schriftliche Einwilligung des AUFTRAGGEBERS Hard- oder Software an die Systeme des AUFTRAGGEBERS anzuschließen oder darauf zu installieren.
7. Dem AUFTRAGNEHMER ist es nicht gestattet, personenbezogene Daten in Systeme Dritter einzuspielen. Dies gilt auch für Testzwecke.
8. Dem AUFTRAGNEHMER ist es nicht gestattet während der Entwicklung von Software oder der Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen des AUFTRAGGEBERS personenbezogenen Daten des AUFTRAGGEBERS zu verwenden. Hierfür sind fiktive Testdaten oder nach ausdrücklicher schriftlicher Einwilligung durch den AUFTRAGGEBER anonymisierte Originaldaten zu verwenden.
9. Zum Schutz personenbezogener Daten vor Missbrauch und Verlust (Datensicherheit) wird der AUFTRAGNEHMER die technischen und organisatorischen Maßnahmen treffen, auf die sich die Parteien entsprechend in Teil 3 der DuD-B TOM, verständigt haben.
10. Die vereinbarten Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung und sind vom AUFTRAGNEHMER dem aktuellen Stand der Technik anzupassen. Dies gilt ebenso im Fall von Anordnungen der zuständigen Aufsichtsbehörden. Beabsichtigte wesentliche Änderungen (z.B. wesentliche Änderung von Verschlüsselungsverfahren oder Anmeldeprozeduren) sind zu dokumentieren und dem AUFTRAGGEBER mitzuteilen sowie einvernehmlich in einer geänderten Fassung des Teil 3 der DuD-B, der „Vereinbarung zur Festlegung der technischen und organisatorischen Maßnahmen“ festzuhalten, wobei der AUFTRAGGEBER Änderungen nicht ohne erheblichen Grund widerspricht.

§ 8 Ermöglichung von Kontrollen und Zurverfügungstellung von Informationen

1. Der AUFTRAGNEHMER erklärt sich damit einverstanden, dass der AUFTRAGGEBER berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen in einem dem Risiko angemessenen Umfang selbst oder durch Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort. Der AUFTRAGNEHMER sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen mitwirkt. Entstehende Kosten bei der Durchführung der Kontrollen werden nicht erstattet.
2. Der AUFTRAGNEHMER gewährleistet die ordnungsgemäße Durchführung der technischen und organisatorischen Maßnahmen (Teil 3 der DuD-B, „TOM“). Die Einhaltung der technischen und organisatorischen Maßnahmen wird der AUFTRAGNEHMER regelmäßig durch geeignete Nachweise z.B. von seiner Revision, seinem betrieblichen Datenschutzbeauftragten oder einer anerkannten Wirtschaftsprüfungsgesellschaft, belegen (Einhaltungsbestätigung).
3. Die Einhaltungsbestätigung oder qualifizierte Prüfungsbestätigung zur Einhaltung des Datenschutzes (z.B. Prüfberichte nach IDW PS 951 mit angemessenen Aussagen zum Datenschutz) ist vom AUFTRAGNEHMER dem AUFTRAGGEBER vor Beginn der Datenverarbeitung und danach sofern im Einzelfall nichts Anderes vereinbart wird,

unaufgefordert jährlich vorzulegen bzw. bereitzustellen. Unabhängig davon räumt der AUFTRAGNEHMER dem AUFTRAGGEBER und dessen Bevollmächtigten bezüglich der vereinbarten technischen und organisatorischen Maßnahmen ein Besichtigungs-, Einsichtnahme-, Auskunfts- und Kontrollrecht (Prüfungsrechte), grundsätzlich nach vorheriger Abstimmung mit dem AUFTRAGNEHMER und während dessen gewöhnlichen Geschäftszeiten, ein. Der AUFTRAGNEHMER ist verpflichtet, im Falle von Auskünften und Einsichtnahmen die erforderliche Unterstützung bereitzustellen. Im Übrigen wird der AUFTRAGNEHMER den Personen, die Prüfungen oder sonstige Maßnahmen vornehmen, den Zugang zu allen Räumlichkeiten und Liegenschaften zwecks Einhaltung der gesetzlichen Prüfpflichten des AUFTRAGGEBERS gewähren.

Teil 3

Vereinbarung zur Festlegung der technischen und organisatorischen Maßnahmen (TOM)

Der AUFTRAGNEHMER trifft geeignete technische und organisatorische Maßnahmen (Art. 32 DS-GVO), um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten.

Diese Maßnahmen schließen folgendes ein:

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

Zutrittskontrolle
Maßnahmen die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden verwehren:

- Elektronisch schlüsselgestützte personalisierte Zutrittskontrollsysteme mit Zutrittsberechtigung nur für autorisierte Mitarbeiter.
- Organisationsanweisung zur Ausgabe von Schlüsseln.
- Verschluss von Laptops in Schränken nach Dienstschluss.
- Abschließen des Gebäudes nach Arbeitsschluss.
- Keine Server oder Serverräume in Büroräumlichkeiten vorhanden.

Zugangskontrolle
Maßnahmen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Serversysteme nur über eine mindestens per verschlüsselte TLS 1.2 Verbindung mit Public Key und Passphrase von autorisierten Mitarbeitern administrierbar.
- Clientsysteme nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar.
- Sperrung des Benutzerkontos nach sechs fehlgeschlagenen Anmeldeversuchen.
- Automatische, passwortgeschützte Bildschirm- und Rechnersperre nach 1 Minute.
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern.
- Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passwörtern.
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware.
- Organisationsanweisung zur Ausgabe von Schlüsseln.
- Verschluss von Laptops in Schränken nach Dienstschluss.
- Abschließen des Gebäudes nach Arbeitsschluss.
- Keine Server oder Serverräume in Büroräumlichkeiten vorhanden.

Zugriffskontrolle
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 nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Die Systeme wurden in der Weise konfiguriert, dass ein regulärer Zugriff mit eingeschränkten Rechten nur für interne, autorisierte Mitarbeiter möglich ist. Vollzugriffs- bzw. Administratorrechte haben nur wenige autorisierte Mitarbeiter über einen gesicherten Bastion-Host / Jump-Server.
- Benutzerberechtigungen müssen zunächst vom jeweiligen Vorgesetzten bewilligt werden, bevor Sie technisch durch die IT eingerichtet werden.
- Verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch IT-Abteilung auf Anweisung des Abteilungsleiters oder der Geschäftsleitung).

Trennungskontrolle
Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Die durch den AUFTRAGNEHMER getroffenen Maßnahmen zur Trennungskontrolle sind der softwareseitige Ausschluss im Sinne einer Mandantentrennung, die Trennung von Test- und Routineprogrammen, sowie Dateiseparierung.
- Beispielsweise müssen alle Produktivsysteme getrennt von den Entwicklungs- und Testsystemen betrieben werden. Technisch wird dieses durch eine Segmentierung von Netzen mit einem aktivierten Firewall-Regelwerk realisiert. Produktivdaten dürfen nicht als Kopie für Testzwecke verwendet werden, ebenso dürfen Testdaten nicht in Produktivumgebung eingesetzt werden.

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:

- Beim Einsatz von Kundendatenbeständen für IT-Softwaretests werden personenbezogene Daten (z.B. E-Mail-Adressen) durch eine Fantasieadresse ersetzt – pseudonymisiert.
- Für eine Aufbewahrung nach Ablauf der Löschfrist sind personenbezogene Daten zu anonymisieren bzw. pseudonymisieren.

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

Weitergabekontrolle
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:

- Die Weitergabe von Daten erfolgt über dedizierten Standleitungen bzw. verschlüsselten VPN-Tunneln.
- Eine E-Mail-Transport-Verschlüsselung wird, sofern beidseitig verfügbar, eingesetzt.
- Der Zugang zu datenverarbeitenden Systemen erfolgt ausschließlich über verschlüsselte Verfahren z.B. OpenSSH oder SSL mit dem Mindeststandart TLS 1.2.
- Eine Bereitstellung von personenbezogenen Daten erfolgen über verschlüsselte Verbindungen wie sftp, OpenSSH oder https mit dem Mindeststandart TLS 1.2.
- Unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung sowie beim Datentransfer wird durch eine Datenverschlüsselung verhindert.

Eingabekontrolle
Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Die Eingabe, Veränderung und Löschung von Daten wird protokolliert.
- Die Vergabe von Rechten zur Eingabe, Veränderung und Löschung von Daten erfolgt grundsätzlich auf Basis des Minimalprinzips durch den Dienst-Administrator.
- Durch die Einhaltung der oben aufgeführten Regeln zu Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle wurde die Grundlage für die Eingabekontrolle der Systeme geschaffen, die personenbezogenen Daten verarbeiten.

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

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit
Maßnahmen die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

- Die Speicherung von Kundendaten erfolgt in den dafür vorgesehenen Rechenzentren der AUFTRAGNEHMER. Eine Speicherung außerhalb dieser ist nicht vorgesehen.
- Vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Datenträger.
- Die Sicherung personenbezogener Daten erfolgt nach Datensicherungskonzepts bzw. entsprechend zusätzlicher Anforderungen. Die Sicherungsvorgänge werden regelmäßig kontrolliert.
- Ein Notfallplan regelt die Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs.

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

Datenschutz-Management

- Der AUFTRAGNEHMER hat einen internen Datenschutzbeauftragten und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Alle Mitarbeiter werden zur Einhaltung der internen Richtlinie zur Datenschutzorganisation geschult und verpflichtet.
- Die Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz steht allen Mitarbeitern bei Bedarf zentral zur Verfügung.
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

- Löschungen in den für die Verarbeitung eingesetzten Systemen können durchgeführt werden (Löschfähigkeit).
- Es werden nur die gemäß Vorgaben des Auftraggebers erforderlichen Daten verarbeitet.
- Es wird sichergestellt, dass Voreinstellungen der Systemlieferanten dahingehend angepasst werden, dass eine Verarbeitung von personenbezogenen Daten nach dem Minimalprinzip nur den notwendigen Personen zugänglich sind und verarbeitet werden.

Auftragskontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Der AUFTRAGNEHMER verarbeitet personenbezogene Daten ausschließlich nach vertraglich getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des AUFTRAGGEBERS. Eine hiervon abweichende Verarbeitung erfolgt nur nach schriftlicher Einwilligung des AUFTRAGGEBERS.
- Der Vertrag enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des AUFTRAGGEBERS sowie ein Verbot der Nutzung durch den AUFTRAGNEHMER außerhalb des schriftlich formulierten Auftrags.
- Eine Überprüfung des Auftragnehmers und seiner Tätigkeiten findet im Rahmen der regelmäßigen internen Audits statt.

Die Datenverarbeitung findet in Deutschland statt. Die im Rechenzentrum umgesetzten technischen und organisatorischen Maßnahmen der Amazon Web Services Inc. (AWS) können unter https://aws.amazon.com/compliance/data-center/data-centers/ und https://aws.amazon.com/compliance/data-center/controls/ eingesehen werden.