Vertrag
über die Verarbeitung von Daten im Auftrag

1. Allgemeines

(1) Der Anbieter verarbeitet personenbezogene Daten im Auftrag des Kunden i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Kunden

(1) Der Kunde ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Anbieter. Dem Anbieter steht nach Ziff. 4 Abs. 5 das Recht zu, den Kunden darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Kunde ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Anbieter wird den Kunden unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Anbieter geltend machen.

(3) Der Kunde hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Anbieter zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Kunden beim Anbieter entstehen, bleiben unberührt.

(5) Der Kunde kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Kunden ändern, wird der Kunde dies dem Anbieter in Textform mitteilen.

(6) Der Kunde informiert den Anbieter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Anbieter feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Kunden geltenden gesetzlichen Meldepflicht besteht, ist der Kunde für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Anbieters

(1) Der Anbieter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Kunden erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Anbieter ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Anbieter dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Kunden. Eine hiervon abweichende Verarbeitung von Daten ist dem Anbieter untersagt, es sei denn, dass der Kunde dieser schriftlich zugestimmt hat.

(2) Der Anbieter verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(3) Der Anbieter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Anbieter ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Kunden verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Anbieter wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Kunden abstimmen.

(5) Der Anbieter wird den Kunden unverzüglich darüber informieren, wenn eine vom Kunden erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Anbieter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Kunden bestätigt oder geändert wird. Sofern der Anbieter darlegen kann, dass eine Verarbeitung nach Weisung des Kunden zu einer Haftung des Anbieters nach Art. 82 DSGVO führen kann, steht dem Anbieter das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Der Anbieter wird die Daten, die er im Auftrag für den Kunden verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(7) Der Anbieter kann dem Kunden die Person(en) benennen, die zum Empfang von Weisungen des Kunden berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Anbieter ändern, wird der Anbieter dies dem Kunden in Textform mitteilen.

5. Datenschutzbeauftragter des Anbieters

(1) Der Anbieter bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Anbieter trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Anbieter wird dem Kunden den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann entfallen, wenn der Anbieter gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen

und der Anbieter nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Kunden gewährleisten.

6. Meldepflichten des Anbieters

(1) Der Anbieter ist verpflichtet, dem Kunden jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Kunden, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Anbieter im Auftrag des Kunden verarbeitet.

(2) Ferner wird der Anbieter den Kunden unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Anbieter tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Anbieter im Auftrag des Kunden erbringt, betreffen kann.

(3) Dem Anbieter ist bekannt, dass für den Kunden eine Meldepflicht im Falle von Datenschutzverletzungen nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Anbieter wird den Kunden bei der Umsetzung der Meldepflichten unterstützen. Der Anbieter wird dem Kunden insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Anbieters an den Kunden muss insbesondere folgende Informationen beinhalten:

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

7. Mitwirkungspflichten des Anbieters

(1) Der Anbieter unterstützt den Kunden bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Anbieter wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Kunden mit. Er hat dem Kunden die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Anbieter unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

(1) Der Kunde hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Kunden durch den Anbieter jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Anbieter ist dem Kunden gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Kunde kann eine Einsichtnahme in die vom Anbieter für den Kunden verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Kunde kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Anbieters zu den jeweils üblichen Geschäftszeiten vornehmen. Der Kunde wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Anbieters durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Anbieter ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Kunden i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Kunden zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Kunde ist über entsprechende geplante Maßnahmen vom Anbieter zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Anbieter ist zulässig. Der Anbieter wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu diesem Vertrag angeben.

(2) Der Anbieter hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Kunde und Anbieter getroffenen Vereinbarungen einhalten kann. Der Anbieter hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Anbieter zu dokumentieren und auf Anfrage dem Kunden zu übermitteln.

(3) Der Anbieter ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Anbieter den Kunden hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

(4) Der Anbieter hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Kunden auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Anbieter hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Anbieter

dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Kunde und Anbieter festgelegt sind. Dem Kunden ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Anbieter ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Kunden und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Kunde und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Anbieter bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Anbieter für den Kunden erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Anbieter ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Kunden genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Kunden verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Der Anbieter ist bei der Verarbeitung von Daten für den Kunden zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Anbieter verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Kunden obliegen. Der Kunde ist verpflichtet, dem Anbieter etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Anbieter sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Anbieter sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Anbieter sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Kunden informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Kunden auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

(1) Der Kunde ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Anbieter ist verpflichtet, den Kunden bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Anbieter hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Kunden erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Anbieters für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Kunden erforderlich ist, wird der Anbieter die jeweils erforderlichen Maßnahmen nach Weisung des Kunden treffen. Der Anbieter wird den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Kunden beim Anbieter entstehen, bleiben unberührt.

(4) Für den Fall, dass ein Betroffener seine Rechte nach den Art. 12-23 DSGVO beim Anbieter geltend macht, obwohl dies offensichtlich eine Verarbeitung personenbezogener Daten betrifft, für die der Kunde verantwortlich ist, ist der Anbieter berechtigt, dem Betroffenen mitzuteilen, dass der Kunde der Verantwortliche für die Datenverarbeitung ist. Der Anbieter darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln. Keine Partei ist berechtigt, diese Informationen Dritten zugänglich zu machen. Eine anonymisierte Nutzung der Informationen ohne Möglichkeit des Rückschlusses auf personenbezogene Daten ist auch nach Ende des Vertrages beiden Parteien erlaubt.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Vergütung

Die Vergütung des Anbieters wird gesondert vereinbart.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Anbieter verpflichtet sich gegenüber dem Kunden zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Anbieter im Voraus mit dem Kunden abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Anbieter ohne Abstimmung mit dem Kunden umgesetzt

werden. Der Kunde kann jederzeit eine aktuelle Fassung der vom Anbieter getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Anbieter wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Anbieter den Kunden informieren.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

(2) Er ist mit einer Frist von 14 Tagen zum Ende des laufenden Monats kündbar.

(3) Der Kunde kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Anbieters gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Anbieter eine Weisung des Kunden nicht ausführen kann oder will oder der Anbieter den Zutritt des Kunden oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Anbieter sämtliche in seinen Besitz gelangten Unterlagen und persönlichen Daten die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Kunden an diesen als Datenbankexport zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren und erfolgt innerhalb von 30 Tagen unwiderruflich. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Kunden gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Kunden unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) Der Kunde hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Unterlagen und personenbezogenen Daten beim Anbieter zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Anbieters erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Kunden angekündigt werden.

(3) Der Anbieter darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit dem Anbieter eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Anbieter i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

18. Schlussbestimmungen

(1) Sollte das Eigentum des Kunden beim Anbieter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Anbieter den Kunden unverzüglich zu informieren. Der Anbieter wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Anbieter bietet folgende allgemeine Arbeiten und/oder Leistungen, die gemäß des Auftrags des Kunden ganz oder nur teilweise in Anspruch genommen werden. Die vom Kunden genutzten Arbeiten und/oder Leistungen werden gesondert vereinbart:

Einrichtung, Bereitstellung und Wartung einer cloud-basierten Softwareinstanz für die digitale Unterstützung des Direktvermarktungsprozesses von physischen Produkten. Die allgemeine Leistung der Softwareinstanz umfasst: Webshop, Kundenauftragsverwaltung, Warenwirtschaftssystem, Kommissionierung, Tourenplanung und –führung, Lieferschein- und Abrechnungserstellung, Zahlungsabgleich, Mahnwesen, Bereitstellung von Finanzdaten für eine betriebliche Umsatzsteuervoranmeldung, Bereitstellung von Verkaufsdaten für betriebliche Kontrollmeldungen sowie informatorische Auswertungsfunktionalitäten der erfassten Daten.

Für Auswertungs- und Support-Zwecke, bei Fehlermeldungen oder durchzuführender Softwarepflege wird über eine gesicherte Verbindung auf die bereitgestellte Softwareinstanz zugegriffen.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Nutzer: Name, Vorname, E-Mail-Adressen, Sprache, Organisation, Adressen, Bankdaten, Steuerdaten, Telefonnummern, Zugriffszeiten

Kunde: Name, Vorname, E-Mail-Adressen, Organisation, Telefonnummern, Rechnungs- und Lieferadresse, Bankdaten, Zahlungsdaten, Steuerdaten, Bestelldaten, Webshop-Nutzerkennung, Zugriffszeiten

Fahrer: Name, Vorname, E-Mail-Adressen, Sprache, Organisation, Telefon, GPS-Ortungsdaten, Zugriffszeiten

3. Kategorien betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:

Arbeitnehmer, Zeitarbeitskräfte, Auszubildende, Hilfskräfte, Kunden, Dienstleister

Anlage 2 - Unterauftragnehmer

Der Anbieter nimmt für die Verarbeitung von Daten im Auftrag des Kunden Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

Amazon Web Services EMEA SARL
38 Avenue John F. Kennedy,
L-1855, Luxemburg,
z. Hd. AWS EMEA Legal
Leistungen: Hosting & Infrastruktur

Graphhopper GmbH
Lindenschmitstr. 52
81373 München
Tel.: +49 89 2500 771 90
Mail: support@graphhopper.com
Leistungen: Geocoding, Distanzmatrix und Optimierung der Tourenplanung

Google Ireland Limited
Gordon House
Barrow Street
Dublin 4
Irland
Tel: +353 1 543 1000
Fax: +353 1 686 5660
E-Mail: support-deutschland@google.com
Leistungen: Kartendarstellung, Routenführung, Geocoding

Anlage 3 - Technische und organisatorische Maßnahmen des Anbieters

Der Anbieter trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Zutrittskontrolle

Der Anbieter gewährleistet durch geeignete Maßnahmen, dass Unbefugten der Zugang zu den Datenverarbeitungsanlagen, auf der die personenbezogenen Daten verarbeitet oder genutzt werden, verwehrt wird. Dies geschieht durch:

- Persönliche Überwachung im Eingangsbereich
- Schlüsselvergabe ausschließlich an autorisierte Personen
- Zutritt zum Gebäude und allen relevanten Räumen nur für Berechtigte, d.h. die jeweiligen Mitarbeiter, Besucher nur in Begleitung von berechtigten Mitarbeitern.
- Zutritt zum abgeschlossenen EDV-Verteiler und Router/Firewall ist nur für autorisierte Mitarbeiter mit Zugangskontrolle

Zugriffskontrolle

Der Anbieter gewährleistet, dass die zur Nutzung seiner Datenverarbeitungssysteme Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten ohne Berechtigung nicht gelesen, kopiert, geändert oder entfernt werden können. Dies geschieht durch:

- Freigabe von Daten nur an berechtigte Personen
- Unterweisung unter Berücksichtigung der individuellen Zugriffsrechte auf personenbezogenen Daten
- Schutz gegen unberechtigte interne und externe Zugriffe durch Firewall bestehen.

Trennung der Verarbeitung für verschiedene Zwecke

Der Anbieter gewährleistet durch geeignete Maßnahmen, dass personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können. Dies geschieht durch:

- Funktionstrennung
- Getrenntes Produktions-und Testsystem
- Getrennte Verarbeitung zweckgebundener Daten

Eingabekontrolle

Der Anbieter ergreift geeignete Maßnahmen, um zu gewährleisten, dass überprüft und sichergestellt werden kann, dass keine personenbezogenen Daten in die Datenverarbeitungssysteme zusätzlich eingegeben oder aus diesen endgültig entfernt worden sind. Dies geschieht durch:

- Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles)
- Der Zugriff auf Datenbestände erfolgt anhand Berechtigungen. Das Verfahren gewährleistet, dass keine Datenveränderungen unbemerkt vorgenommen werden können.

Weitergabekontrolle

Der Anbieter verhindert durch geeignete Maßnahmen, dass bei der Übertragung der personenbezogenen Daten sowie bei Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Dies geschieht durch:

- Einsatz aktueller Firewall
- E-Mail Nachrichten bzw. sonstige Informationen werden verschlüsselt versendet
- Einsatz von Verschlüsselungstechnologien für Dokument und VPN-Technologie (SSL/TLS) zur Datenkommunikation

Auftragskontrolle

Der Anbieter sichert durch geeignete Maßnahmen, dass in Fällen der Auftragsdatenverarbeitung personenbezogene Daten im Einklang mit den Weisungen des Kunden verarbeitet werden. Dies geschieht durch:

- Eindeutige Vertragsgestaltung
- Kontrolle der Vertragsausführung
- Klare Anweisungen an den Anbieter hinsichtlich des Umfangs der Verarbeitung personenbezogener Daten.
- Soweit eine Datenverarbeitung im Auftrag durchgeführt wird, wird der Anbieter vor Aufnahme der Datenverarbeitung nach den Vorschriften der DSGVO auf die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen überprüft. Über jeden Auftrag wird ein Vertrag nach den Vorschriften der Datenschutz-Grundverordnung abgeschlossen. Dies gilt auch für Verträge über Wartungsarbeiten an den Datenverarbeitungssystemen und Softwarepflege je nach Bedarf und sonstige IT Service-Unterstützung, wenn dabei ein Zugriff auf personenbezogenen Daten nicht ausgeschlossen werden kann.

Organisationskontrolle

Für die Verarbeitung von Daten beim Anbieter sind Prozesse und Arbeitsabläufe definiert, die Umsetzung und Einhaltung der Prozesse werden kontrolliert. Die Mitarbeiter des Anbieters werden in folgenden Punkten geschult/verpflichtet:

- Grundsätze des Datenschutzes und der IT-Sicherheit
- Pflicht zur Verschwiegenheit über Betriebs-und Geschäftsgeheimnisse
- Ordnungsgemäßer und sorgfältiger Umgang mit Daten, Dateien, Datenträgern und sonstigen Unterlagen
- Der Anbieter gewährleistet, dass die Leistungserbringung unter Beachtung des Datenschutzrechts erfolgt.