CleverOne Vereinbarung Auftragsverarbeitung

1. Allgemeines

Der Auftragnehmer stellt dem Auftraggeber seine All-in-One-SaaS-Plattform für das Management von Bestattungsunternehmen als Software as a Service (SaaS) zur Verfügung. Mit der Software kann der Auftraggeber personenbezogene Daten erheben und verarbeiten. Dementsprechend beinhaltet der von den Parteien geschlossene Vertrag über die Zurverfügungstellung der Software („Hauptvertrag“) die Verarbeitung von personenbezogenen Daten im Auftrag durch den Auftragnehmer. Diese Vereinbarung über eine Auftragsverarbeitung („AVV“) konkretisiert, als Teil des Hauptvertrages, die Verpflichtungen beider Parteien zur Einhaltung des anwendbaren Datenschutzrechts, insbesondere der Anforderungen der Datenschutz-Grundverordnung („DSGVO“).

2. Anwendungsbereich

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind im Hauptvertrag und in **Anhang 1 zu dieser AVV** festgelegt. Die Laufzeit dieser AVV und die Dauer der Auftragsverarbeitung entsprechen der Laufzeit des Hauptvertrages.

3. Weisungsgebundenheit

3.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Dies betrifft auch die Übermittlung in Drittländer ohne angemessenes Datenschutzniveau. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in Textform geändert, ergänzt oder ersetzt werden. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

3.2 Falls der Auftragnehmer nach dem Recht der Union oder des Mitgliedstaates, dem der Auftragnehmer unterliegt, verpflichtet ist, personenbezogene Daten zu verarbeiten, wird der Auftragnehmer den Auftraggeber hierüber vor der jeweiligen Verarbeitung schriftlich informieren, es sei denn, das Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses. Im letztgenannten Fall wird der Auftragnehmer den Verantwortlichen unverzüglich informieren, sobald ihm dies rechtlich möglich ist.

3.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.4 Der Auftragnehmer darf Daten über die Nutzung der Software durch den Auftraggeber in anonymisierter Form zum Zwecke der Optimierung der Software, der User Experience und für sicherheitsrelevante Auswertungen verwenden. Der Auftraggeber erteilt hiermit eine entsprechende Weisung für die entsprechende Anonymisierung.

4. Technische und organisatorische Maßnahmen

4.1 Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

4.2 Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist in **Anhang 2 zu dieser AVV** dokumentiert. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und

organisatorischen Maßnahmen erforderlich werden können. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftraggeber kann jederzeit eine aktuelle Übersicht der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

5. Betroffenenrechte

5.1 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO (insb. Auskunft, Berichtigung, Sperrung oder Löschung). Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

5.2 Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

6. Sonstige Pflichten des Auftragnehmers

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

6.2 Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie erforderlichenfalls bei Durchführung einer Datenschutzfolgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind dem Auftraggeber auf Anforderung unverzüglich zur Verfügung zu stellen.

6.3 Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

6.4 Die beim Auftragnehmer zur Verarbeitung eingesetzten Personen haben sich schriftlich zur Vertraulichkeit verpflichtet, wurden mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht und werden hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht.

6.5 Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützen.

7. Rechte und Pflichten des Auftraggebers

7.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

7.2 Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, die mit dem Auftragnehmer nicht im Wettbewerb stehen, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer, soweit erforderlich und möglich, Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer

Kontrolle erforderlich sind. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

8. Unterauftragsverarbeiter

8.1 Die Beauftragung von Unterauftragsverarbeitern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers zulässig. Der Auftraggeber stimmt der Beauftragung von Unterauftragsverarbeitern gemäß der Übersicht Unterauftragsverarbeiter, anbei als **Anhang 3 zu dieser AVV**, zu. In der Übersicht Unterauftragsverarbeiter ist auch der Prozess für zukünftige Änderungen der Unterauftragsverarbeiter definiert.

8.2 Der Auftragnehmer hat die Unterauftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass diese die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten können. Der Auftragnehmer hat insbesondere zu kontrollieren, dass sämtliche Unterauftragsverarbeiter die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen haben.

8.3 Nicht als Unterauftragsverarbeitung im Sinne dieser AVV sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben.

8.4 Die Beauftragung von Unterauftragsverarbeitern lässt die vertraglichen und datenschutzrechtlichen Verpflichtungen des Auftragnehmers gegenüber dem Auftraggeber unberührt. Der Auftragnehmer haftet für eventuelle Schlechtleistungen eines Unterauftragsverarbeiters wie für eigenes Verschulden.

9. Löschung und Rückgabe von personenbezogenen Daten

9.1 Kopien oder Duplikate der Daten 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.

9.2 Nach Beendigung der Leistungsvereinbarung oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer die im Auftrag verarbeiteten personenbezogenen Daten dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen. Eine Löschung der Daten erfolgt automatisiert 4 Wochen nach Beendigung der Leistungsvereinbarung.

9.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

10. Schlussbestimmungen

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

Anlage 1 zur Vereinbarung Auftragsverarbeitung: Beschreibung der Auftragsverarbeitung

1. Gegenstand, Art und Zweck der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber seine All-in-One-SaaS-Plattform für das Management von Bestattungsunternehmen als SaaS-Lösung zur Verfügung. Er wird dabei als Auftragsverarbeiter für den Auftraggeber tätig. Der im Hauptvertrag bezeichnete Auftraggeber ist Verantwortlicher im Sinne der DSGVO und nutzt die SaaS-Plattform des Auftragnehmers zur Erhebung und Verarbeitung personenbezogener Daten.

2. Betroffene Personen

Die im Auftrag verarbeiteten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

- Derzeitige und frühere Mitarbeiter des Auftraggebers
- Derzeitige und frühere Mitarbeiter von Dienstleistern des Auftraggebers
- Interessenten und Kunden des Auftraggebers und deren Angehörige

3. Kategorien von Daten

Die im Auftrag verarbeiteten personenbezogenen Daten gehören zu folgenden Datenkategorien:

- Stammdaten von Mitarbeiter des Auftraggebers und deren Dienstleister: Name, Vorname, Titel, Arbeitgeber, E-Mail-Adresse
- Vertragsdaten von Mitarbeitern des Auftraggebers und von Mitarbeitern von Dienstleistern des Auftraggebers einschließlich Disposition und Urlaubsansprüche
- Bei Nutzung der App GPS-Tracking/Geolokalisierung der Mitarbeiter des Auftraggebers
- Name, Vorname, Anschrift, Geburtsdaten, Bilder, Videos, von Interessenten und Kunden des Auftraggebers und von deren Angehörigen
- Vertrags- und Abrechnungsdaten, angefragte bzw. in Anspruch genommene Leistungen der Kunden des Auftraggebers bzw. von deren Angehörigen

4. Dauer der Auftragsverarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrages.

Anlage 2 zur Vereinbarung Auftragsverarbeitung: Technische und organisatorische Maßnahmen

1. Vertraulichkeit

1.1 Zutrittskontrolle

Hosting/Rechenzentrum:

Das Hosting der Server wird von AWS in Frankfurt am Main bereitgestellt. Der Zugang wird per Vereinzelungsanlage sichergestellt. Weiterhin ist das gesamte Gelände außerhalb und innerhalb der Rechenzentren durch Videoüberwachung und 365x7x24 Sicherheitspersonal geschützt.

Details: https://aws.amazon.com/de/compliance/data-center/controls

Büroräume:

Die Büroräume des Auftragnehmers befinden sich in einem Bürohaus. Die Zugänge zum Bürohaus und auch zu den Büroräumen des Auftragnehmers sind während der Bürozeiten dauerhaft besetzt und während der Nacht verschlossen. Zugang zu dem Bürohaus haben nur der Vermieter und die Mieter der Büroräume. Es kommt ein Schließsystem zum Einsatz, das vom Vermieter verwaltet wird. Jeder Mieter des Bürohauses hat jedoch die Möglichkeit, die jeweils ausgehändigten Schlüssel selbst zu verwalten und Zutrittsrecht zu erteilen und zu entziehen. Dies wird von der Personalabteilung des Auftragnehmers verwaltet.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher können den Empfang betreten, erhalten erst Zutritt zu den Büroräumen nach vorheriger Anmeldung.

Jeder Besucher wird von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet.

Die Büroräume sind am Tag als auch in der Nacht per Videoaufzeichnung überwacht. Die Besucher werden per Hinweis darüber aufgeklärt. Die Aufbewahrung erfolgt nach den Vorgaben der DSGVO.

1.2 Zugangskontrolle

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Die Vergabe und Änderung von Benutzerberechtigungen unterliegt einer Passwortrichtlinie, die unter anderem die Wiederverwendung von Passwörtern verhindert.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei mehrmaliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte SSL-Verbindungen.

Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

1.3 Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden ausschließlich von Administratoren eingerichtet.

Berechtigungen werden nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind. Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Beschäftigten ist es grundsätzlich untersagt und auch per Richtline nicht möglich, nicht genehmigte Software auf den IT-Systemen zu installieren.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

1.4 Trennung

Alle vom Auftragnehmer für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die logische Zuordnung der im Auftrag eines Kunden verarbeiteten Daten zu dem jeweiligen Kunden und damit die logische Trennung der Daten ist stets gewährleistet.

1.5 Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

2. Integrität

2.1 Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die vom Auftragnehmer im Auftrag verarbeitet werden, wird protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

2.2 Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden des Auftragnehmers erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten des Auftragnehmers untersagt.

Mitarbeiter des Auftragnehmers werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

3. Verfügbarkeit und Belastbarkeit

Die Daten auf den Servern beim Hosting Provider AWS werden täglich als Full Backup gesichert.

Die Daten auf den internen Systemen des Auftragnehmers werden täglich inkrementell und monatlich als Full Backup per eigenem VLAN gesichert. Die Sicherungsmedien werden verschlüsselt an einen

physisch getrennten Ort gespeichert. Der Backupserver befindet sich in einem separatem Brandschott. Das Einspielen von Backups wird regelmäßig getestet.

Die Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Rechenzentrum befindet sich eine Brandmeldeanlage sowie eine Löschanlage. Alle Systeme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Es besteht ein Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

4. Auftragskontrolle

Die Software des Auftragnehmers wird in der Europäischen Union gehostet.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des Art. 28 DSGVO ein Auftragsverarbeitungsvertrag nach zuvor durchgeführtem Audit abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

5. Privacy by Design und Privacy by Default

Es wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit Rechnung getragen wird. Die Art der Datenerhebung mittels der Software und die zu erhebenden Datenkategorien können vom Auftraggeber individuell angepasst und verwaltet werden.

Die Software des Auftragnehmers unterstützt die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen auf Daten oder Applikationen können gesetzt werden.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Auftragnehmer hat ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt. Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

Anlage 3 zur Vereinbarung Auftragsverarbeitung:
Übersicht Unterauftragsverarbeiter

Der Auftragnehmer setzt bei der Erbringung der Leistungen aus dem Hauptvertrag folgende Unterauftragsverarbeiter ein:

Unterauftragsverarbeiter	Leistungen des Unterauftragsverarbeiter	Ort der Datenverarbeitung
Amazon Web Services EMEA SARL (Luxemburg)	Hosting der Software	Deutschland EU-Central-1
SevDesk GmbH (Deutschland)	Zurverfügungstellung des Moduls Buchhaltungsfunktionalität	Deutschland
Nur wenn das Modul „Kündigungsservice“ in Anspruch genommen wird:		
Aboalarm GmbH (Deutschland)	Zurverfügungstellung des Moduls Kündigungsservice für die Erstellung und Übermittlung von Kündigungen	Deutschland
Nur wenn das Modul „Factoring“ in Anspruch genommen wird:		
Adelta.Finaz AG (Deutschland)	Factoring Dienstleistungen	Deutschland
abcfinance advise GmbH (Deutschland)	Factoring Dienstleistungen	Deutschland
Nur wenn das Modul „Trauerdruck“ in Anspruch genommen wird und nach Service:		
CloudLab Sales & Management GmbH (Deutschland)	Zurverfügungstellung des Moduls Trauerdruck für die Erstellung von Druckvorlagen	Deutschland
medienwerk7 GmbH (Deutschland)	Druckdienstleistungen (Print-on-Demand)	Deutschland
Trauerdruck App (Deutschland)	Erstellung von Druckvorlagen zum Druck inhouse bei Nutzung von BOK Produkten Print-on-Demand	Deutschland
Peka Verlags-GmbH (Deutschland)	Zurverfügungstellung der Module Trauerdruck/Zeitungsanzeigen für die Erstellung von Druckvorlagen	Deutschland

Der Auftragnehmer kann die Beauftragung einzelner Unterauftragsverarbeiter beenden oder zusätzliche Unterauftragsverarbeiter beauftragen.

Der Auftragnehmer wird den Auftraggeber bei der Beauftragung zusätzlicher Unterauftragsverarbeiter auf elektronischem Wege mindestens 30 Tage vor Einsatz des zusätzlichen Unterauftragsverarbeiters über dessen geplanten Einsatz informieren. Ausgenommen hiervon sind Notfallersetzungen wie weiter unten definiert.

Sollte der Auftraggeber einen wesentlichen Grund haben, dem Einsatz eines Unterauftragsverarbeiters zu widersprechen, wird der Auftraggeber dies dem Auftragnehmer spätestens 15 Tage nach der Information über den geplanten Einsatz des Unterauftragsverarbeiters schriftlich und unter Nennung des wesentlichen Grundes mitteilen. Sollte der Auftraggeber innerhalb dieser Zeitspanne nicht widersprechen, so wird der Einsatz des zusätzlichen Unterauftragsverarbeiters als vom Auftraggeber genehmigt angesehen.

Sollte der Auftraggeber widersprechen, kann der Auftragnehmer den Widerspruch wie folgt heilen: (1.) Der Auftragnehmer wird den zusätzlichen Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten des Auftraggebers nicht einsetzen, oder (2.) der Auftragnehmer wird Maßnahmen ergreifen, um den wesentlichen Grund für den Widerspruch des Auftraggebers auszuräumen, oder (3.) der Auftragnehmer kann die Erbringung des von dem Einsatz des zusätzlichen Unterauftragsverarbeiters betroffenen Aspekts der Leistung gegenüber dem Auftraggeber vorübergehend oder dauerhaft einstellen und dem Auftraggeber die für die Erbringung des Aspekts der Leistung eventuell bereits vorab gezahlte Vergütung zurückerstatten. Sollte keine dieser drei Optionen machbar sein und wurde dem Widerspruch nicht innerhalb von 15 Tagen nach Zugang des Widerspruchs abgeholfen, kann jede Partei den Hauptvertrag mit angemessener Frist außerordentlich kündigen.

Notfallersetzungen eines Unterauftragsverarbeiters können erforderlich werden, wenn die Erforderlichkeit des sofortigen Einsatzes eines zusätzlichen Unterauftragsverarbeiters außerhalb der Kontrolle des Auftragnehmers liegt, beispielsweise wenn ein Unterauftragsverarbeiter überraschend den Geschäftsbetrieb einstellt oder seine wesentlichen Vertragspflichten gegenüber dem Auftragnehmer verletzt, so dass es dem Auftragnehmer nicht mehr möglich ist/wäre, die gegenüber dem Auftraggeber geschuldete Leistung zu erbringen. In einem solchen Fall wird der Auftragnehmer den Kunden unverzüglich über den zusätzlichen Unterauftragsverarbeiter informieren und der Widerspruchsprozess, wie oben definiert, wird mit der Information des Auftraggebers eingeleitet.