Verarbeitung personenbezogener Daten im Auftrag
gemäß Art. 28 DSGVO mit Wirkung ab dem 25.5.2018

zwischen
dem **Auftraggeber**, der die Annahme dieser Vereinbarung bestätigt,

und der
expenseBrain GmbH, Lindau
- nachstehend „Auftragnehmer" genannt –
- „Auftraggeber" und „Auftragnehmer" einzeln/gemeinsam nachstehend „Vertragspartner" genannt –

1. Vorbemerkung

Der Auftragnehmer erbringt Beratungsleistungen, die der Organisation des Auftraggebers bzw. seiner Mitarbeiter dienen. Die Leistungen sind nach Leistungsarten gegliedert, u.a. Beratung, Implementierung, Projektmanagement und Training, und enthalten Leistungen, die auch online bzw. über allgemein zugängliche Datennetze erbracht werden können

Der Auftragnehmer versucht die Verarbeitung von produktiven Personaldaten durch Nutzung von Demosystemen oder Anonymisierung bestmöglich zu vermeiden.

Die Leistungen werden auf der Basis des jeweiligen *Auftrages* erbracht. Dem Auftraggeber ist bekannt, dass Leistungen auch durch *Unterauftragnehmer* des Auftragnehmer erbracht werden können.

Im Rahmen der Erbringung von Leistungen für einen *Auftrag* kann es erforderlich sein, dass der Auftragnehmer bzw. die von ihm eingeschalteten *Unterauftragnehmer* mit *personenbezogenen Daten* umgehen, für die der Auftraggeber Verantwortlicher ist. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragspartner im Zusammenhang mit dem Umgang der Auftragnehmerseite mit solchen personenbezogenen Daten. *Personenbezogene Daten* in Form von *Auftraggeber-Daten* werden unter dieser VAV ausschließlich im Auftrag des Auftraggeber verarbeitet.

2. Begriffe

Für die VAV gelten die nachstehend in alphabetischer Reihenfolge aufgeführten und definierten Begriffe; diese werden in Kursivdruck hervorgehoben.

1. ***„Auftraggeber-Daten"*** sind diejenigen gemäß einem *Auftrag* im Auftrag zu *verarbeitenden personenbezogenen Daten*, für die der Auftraggeber *Verantwortlicher* ist.
2. ***„Auftragsverarbeitung"*** (Verbform ***„im Auftrag verarbeiten"***) ist die *Verarbeitung* der *Auftraggeber-Daten* durch den Auftragnehmer, und zwar ausschließlich (i) nach Weisungen des Auftraggeber im Rahmen eines *Auftrags* und dieser VAV sowie der wirksamen Einzelweisungen und (ii) ergänzend im Rahmen der Vorgaben gem. Art. 28, 29 DS-GVO.
3. ***„Besonders schützenswerte personenbezogene Daten"*** (Art. 9 DS-GVO) sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
4. ***„Dritter"*** (Art. 4 Nr. 10 DS-GVO) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der *betroffenen Person*, dem *Verantwortlichen*, dem jeweiligen Auftragnehmer und den Personen, die unter der unmittelbaren Verantwortung des *Verantwortlichen* oder des Auftragnehmers befugt sind, die *Auftraggeber-Daten* zu *verarbeiten*.
5. „***DSB***" ist die Abkürzung für „Datenschutzbeauftragter". Dies ist eine geeignete Person gemäß Art. 37 bis 39 DS-GVO, § 38 BDSG.
6. „***Auftrag***" bezeichnet eine Vereinbarung zwischen den Vertragspartnern über die Erbringung von Leistungen der in Ziff. II.2. bezeichneten Art. Es können mehrere *Aufträge* parallel bestehen. Der *Auftrag* kann u.a. bestehen aus einem Angebot, einer Auftragsbestätigung, einer Leistungsbeschreibung und den AuftraggeberB sowie etwaigen Nachträgen und Zusatzvereinbarungen, jeweils in der anwendbaren Fassung. Die VAV gilt auch, sofern die Leistungsbeschreibungen und die jeweiligen *Aufträge* nicht ausdrücklich Bezug nehmen auf die VAV.
7. ***„Personenbezogene Daten"*** **(**Art. 4 Nr. 1 DS-GVO) sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („*betroffene Person*" genannt) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
8. ***„TOM"*** ist eine Abkürzung für ***„technische und/oder organisatorische Maßnahmen"*** (Art. 28 Abs. 3 S. 2 lit. c), Art. 32 DS-GVO) und meint auf Seiten des Auftragnehmer, sofern nicht ausdrücklich anders beschrie- ben, die in dem Datenschutzkonzept des Auftragnehmer niedergelegten TOM nach Art. 32 DSGVO.

9. „***Unterauftragnehmer***" ist die Abkürzung für „Unterauftragnehmer" und bezeichnet die sog. „weiteren Auftragnehmer" i.S.d. Art. 28 Abs. 2 und 4 DS-GVO. Dies sind Unternehmen oder Personen, die Leistungen im Unterauftrag des Auftragnehmer erbringen, die sich unmittelbar auf die Erbringung einer Hauptleistung gemäß dem anwendbaren *Auftrag* oder der VAV beziehen. Nicht hierzu gehören i.d.R. Nebenleistungen, die z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen durch Dritte erbracht werden.
10. ***„Verarbeitung"*** (Verbform ***„verarbeiten"***) (Art. 4 Nr. 2 DS-GVO) ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vor- gang oder jede solche Vorgangsreihe im Zusammenhang mit *Auftraggeber-Daten* wie Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form von Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung. *Verarbeitung* meint dabei in erster Linie die vollständig oder teilweise automatisierte *Verarbeitung*, aber auch die nicht au- tomatisierte *Verarbeitung* von *Auftraggeber-Daten*, die bereits in einer Datei gespeichert sind oder noch gespeichert werden sollen. *Verarbeitung* erfolgt vonseiten des Auftragnehmers unter einem *Auftrag* nur als *Auftragsverarbeitung*.
11. ***„Verantwortlicher"*** (Art. 4 Nr. 7 DS-GVO) ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der *Verarbeitung* von *personenbezogenen Daten* entscheidet. *Verantwortlicher* unter der VAV bzw. unter einem *Auftrag* ist der Auftraggeber.

3. Art, Umfang, Zweck, Laufzeit der Auftragsverarbeitung

1. Der Auftragnehmer betreibt unter der VAV ausschließlich Auftragsverarbeitung. Der Auftraggeber bleibt Verantwortlicher („Herr der Daten").
2. Die Art der Auftragsverarbeitung umfasst diejenigen Arten von Verarbeitungen, die zur Erbringung der vereinbarten Leistungen gem. dem jeweiligen Auftrag erforderlich sind.
3. Der Auftragnehmer ist ungeachtet der in Ziff. 2 genannten Zwecke berechtigt, die personenbezogenen Daten zu verarbeiten zum Zweck der Bearbeitung von Mängeln oder Störungen, zum Zweck der Qualitätssicherung, soweit der Auftragnehmer dies für die Gewährleistung der Netz- und Informationssicherheit innerhalb des eigenen Leistungsbereiches (insbes. Rechenzentrum) für notwendig und verhältnismäßig erachtet, soweit dadurch die Fähigkeit eines von einem Vertragspartner eingesetzten Netzes oder Informationssystems gewährleistet wird, Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit personenbezogener Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Dies umfasst insbesondere auch, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern und Schädigungen von Informations- und Kommunikationssystemen abzuwehren.

4. Die Art der personenbezogenen Daten sind alle Arten personenbezogener Daten, die ein Auftragnehmer im Auftrag des Auftraggeber verarbeitet. Hiervon umfasst sind gelegentlich auch besonders schützenswerte personenbezogener Daten. Für eine etwa notwendige Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) ist allein der Auftraggeber verantwortlich; der Auftragnehmer leistet insoweit Unterstützung nach Maßgabe der VAV.
5. Hinsichtlich der Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten i.S.d. Art. 10 DS-GVO ist der Auftraggeber verpflichtet, in eigener Verantwortung dafür Sorge zu tragen, dass die hierzu geltenden gesetzlichen Vorgaben eingehalten werden.
6. Kategorien betroffener Personen sind die in dem jeweiligen Auftrag genannten Personenkreise bzw. Kategorien, vorbehaltlich dort getroffener abweichender Bestimmung folgende Kategorien natürlicher Personen:
   - der Auftraggeber selbst, sofern dieser eine natürliche Person ist,
   - Beschäftigte und Geschäftspartner (insbes. Kunden, Lieferanten) des Auftraggeber,
   - Beschäftigte, Familienangehörige und Geschäftspartner (insbes. Kunden und Lieferanten) des Geschäftspartners,
   - Beschäftigte des Geschäftspartners des Geschäftspartners.
7. Die Laufzeit der Auftragsverarbeitung ergibt sich aus dem jeweiligen Auftrag und ist im Zweifel auf die Laufzeit des Auftrages begrenzt. Der Auftragnehmer übergibt bzw. löscht die Auftraggeber-Daten gemäß den Bestimmungen in Ziffer XI.

4. Ort der Auftragsverarbeitung

Die *Auftragsverarbeitung* findet ausschließlich in Deutschland oder in einem Staat der Europäischen Union oder des Europäischen Wirtschaftsraums statt.

Die Verlagerung/ Übermittlung in ein Drittland bedarf der vorherigen dokumentierten Zustimmung des Auftraggeber und darf nur erfolgen, wenn zuvor die besonderen Voraussetzungen der Art. 44 DS-GVO erfüllt sind. Dies erfolgt auf Anforderung des Auftraggeber durch eine Vereinbarung gemäß **Anlage 2** (Vereinbarung der derzeit geltenden EU-Standardvertrags- klauseln Controller/Processor) mit dem Auftraggeber in der Rolle des Datenexporteurs/ Controllers und dem Auftragnehmer in der Rolle des Datenimporteurs/Processors.

Sofern *Unterauftragnehmer* nach Ziff. IX (weitere Auftragsverarbeiter) in einem Drittland tätig sind, wird zwischen dem Auftragnehmer und dem *Unterauftragnehmer* zuvor eine entsprechende Vereinbarung nach **Anlage 2** geschlossen.

5. Weisungsbefugnis des Auftraggebers

Der Auftragnehmer *verarbeitet* die *Auftraggeber-Daten* ausschließlich in Übereinstimmung mit den Weisungen des Auftraggeber, wie sie – vorbehaltlich etwaiger wirksamer Einzelweisungen – abschließend in den Bestimmungen der VAV und im jeweiligen *Auftrag* enthalten sind.

Einzelweisungen, die von den im jeweiligen *Auftrag* getroffenen Festlegungen abweichen oder im Verhältnis dazu zusätzliche bzw. veränderte Anforderungen aufstellen, bedürfen zu ihrer Wirksamkeit mindestens der Textform und, sofern und soweit dadurch beim Auftragnehmer bestehende Arbeitsabläufe verändert werden, sich der Aufwand beim Auftragnehmer erhöht oder der Auftraggeber in der Weisung nicht darlegen kann, dass sich datenschutzrechtliche Risiken für den Auftragnehmer im Verhältnis zu dem jeweils vorangehenden Zustand nicht erhöhen, einer ausdrücklichen vorherigen Zustimmung seitens des Auftragnehmer, mindestens in Textform.

Solche Einzelweisungen erfolgen im Übrigen nach Maßgabe eines etwa im *Auftrag* festgelegten Änderungsverfahrens. Mehraufwand, der durch die Übernahme der Abweichung oder Änderung aufgrund der Weisung des Auftraggebers bedingt sind, gehen zu dessen Lasten.

Eine nicht mindestens in Textform erfolgende Einzelweisung ist unverzüglich in Textform zu bestätigen. Der Auftragnehmer ist berechtigt, die aufgrund einer Weisung geschuldete Tätigkeit auszusetzen, bis die dokumentierte Form der Weisung erfolgt ist.

Eine von wirksamen Weisungen bzw. Einzelweisungen abweichende *Auftragsverarbeitung* ist ausgeschlossen.

Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggeber gegen geltendes Datenschutzrecht verstößt, wird er gemäß Art. 28 Abs. 3 Satz 3 i.V.m. lit. h DS-GVO den Auftraggeber möglichst zeitnah, mindestens in Textform, da- rauf hinweisen. Außerdem ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer dokumentierten Bestätigung der Weisung durch den Auftraggeber auszusetzen.

Folgt der Auftragnehmer nach der Bestätigung der Weisung durch den Auftraggeber der bestätigten Weisung, trägt der Auftraggeber alle damit etwa verbundenen Risiken, insbesondere betreffend der Einhaltung von Datenschutzvorschriften und der Ansprüche *betroffener Personen.* Dies gilt jedoch nicht, sofern und soweit eine von dem Auftragnehmer zu vertretende, inhaltlich fehlerhafte Ausführung der Weisung erfolgt. Der Auftragnehmer übernimmt keine Haftung für die Rechtmäßigkeit der erteilten Aufträge, es sei denn, dass für den Auftragnehmer spezifische Datenschutzvorschriften als Auftragsverarbeiter gelten und von diesem verletzt wurden.

Auf Seiten des Auftraggeber sind ausschließlich diejenigen Personen weisungsbefugt, die ein Benutzerkonto bei dem Auftragnehmer führen, und nur für solche Weisungen, die sie im Rahmen dieses Benutzerkontos erteilen, entweder als *Auftrag* oder als Einzelweisung.

6. Pflichten des Auftraggebers

Der Auftraggeber ist im Rahmen der VAV für die Einhaltung der anwendbaren datenschutzrechtlichen Vorschriften allein verantwortlich, insbesondere für die Zulässigkeit und Rechtmäßigkeit der *Verarbeitung*. Dies gilt nicht, sofern und soweit der Auftragnehmer rechtmäßigen Weisungen des Auftraggebers zuwiderhandelt oder in zu vertretender Weise die für Auftragsverarbeiter anwendbaren Vorschriften des Datenschutzrechts bzw. die VAV verletzt (Art. 82 Abs. 2 S. 2 DS-GVO).

Sollten *Dritte* gegen den Auftragnehmer aufgrund der *Verarbeitung* von *Auftraggeber-Daten* Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen, sofern und soweit nicht Ziff. 1 Satz 2 eingreift.

Der Auftraggeber ist im Verhältnis der Vertragspartner zueinander Berechtigter bzgl. der *Auftraggeber-Daten* und Inhaber aller etwaiger Rechte, die die *Auftraggeber-Daten* betreffen.

Der Auftraggeber ist verpflichtet, dem Auftragnehmer die *Auftraggeber-Daten* rechtzeitig zur Leistungserbringung nach dem jeweiligen *Auftrag* zur Verfügung zu stellen. Der Auftraggeber ist verantwortlich für die Qualität einschließlich der Aktualität und der Richtigkeit der zur Verfügung gestellten *Auftraggeber-Daten*.

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig in dokumentierter Form zu informieren, wenn er bei der Prüfung der Ergebnisse der Tätigkeiten des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seiner Weisungen feststellt.

Der Auftraggeber ist gehalten, etwa übermittelte Protokolle von Leistungen, die sich auf *personenbezogene Daten* beziehen, unverzüglich zu überprüfen. Beanstandungen mit Bezug auf die *Verarbeitung* sind innerhalb von drei (3) *Arbeitstagen* zu melden.

Weitere Pflichten und Rechte des Auftraggeber ergeben sich aus den Regelungen der VAV, der DS-GVO sowie den gesetzlichen Bestimmungen.

7. Pflichten des Auftragnehmers

1. Der Auftragnehmer hat eigene Pflichten gem. Art. 28 bis 33 DS-GVO, i.E.:

a) Er gewährleistet und kontrolliert regelmäßig, dass die *Auftrags- verarbeitung* nach dem *Auftrag* im eigenen Verantwortungsbereich (einschl. *Unterauftragnehmer*) in Übereinstimmung mit der VAV und der gesetzlichen Vorschriften erfolgt.

b) Er darf ohne vorherige dokumentierte Zustimmung des Auftraggeber keine Kopien oder Duplikate der *Auftraggeber-Daten* anfertigen. Hiervon ausgenommen sind Kopien, die zur Gewährleistung einer ordnungsgemäßen *Verarbeitung* und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem jeweiligen *Auftrag* erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

c) Er unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die *Auftragsverarbeitung* betreffen. Den hierbei entstehenden Aufwand trägt der Auftraggeber.

d) Er hat dem Auftraggeber auf Anforderung eine Übersicht über die in Art. 30 Abs. 2 DS-GVO genannten Angaben auszuhändigen.

e) Er setzt zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Personen aufseiten des Auftragnehmer, die Zugang zu *Auftraggeber-Daten* haben, dürfen diese ausschließlich entsprechend der Weisung des Auftraggeber und die VAV *verarbeiten*, es sei denn, dass sie gesetzlich zur *Verarbeitung* verpflichtet sind.

f) Er gewährleistet die Umsetzung und Einhaltung der vereinbarten *TOM*.

g) Die Vertragspartner arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Hierzu leistet der Auftragnehmer die notwendigen Beiträge. Hierdurch entstehenden Aufwand hat der Auftraggeber zu tragen.

h) Er hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maß- nahmen der Aufsichtsbehörde zu informieren, soweit sie sich auf die *Auftragsverarbeitung* beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die *Auftragsverarbeitung* beim Auftragnehmer ermittelt.

i) Soweit der Auftraggeber 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, hat ihn dieser nach besten Kräften zu unterstützen. Den hierbei entstehenden Aufwand trägt der Auftraggeber.

j) Tätigkeiten, die der Verantwortliche im Verhältnis zu *betroffenen Personen* schuldet, z.B. die Umsetzung von Löschkonzepten, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft, sind nur dann und insoweit unmittelbar durch den Auftragnehmer durchzuführen, als sie gemäß dem jeweiligen *Auftrag* vom vereinbarten Leistungsumfang ausdrücklich umfasst sind. Der dadurch anfallende Aufwand wird von dem Auftraggeber gesondert getragen.

Eine Pflicht zur Bestellung eines *DSB* besteht beim Auftragnehmer aufgrund der Unternehmensgröße nicht.

3. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung von dessen in Art. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit von *personenbezogenen Daten*, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Zu den Pflichten gehören für die *Auftragsverarbeitung* u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch die *TOM*, die die Umstände und Zwecke der *Verarbeitung* sowie die b. prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignis- sen ermöglichen,

b) die Verpflichtung, Verletzungen von *Auftraggeber-Daten* unverzüglich an den Auftraggeber zu melden,

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber betroffenen Personen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung des Auftraggebers für eine von diesem etwa vorzunehmende Datenschutz-Folgenabschätzung,

e) die Unterstützung des Auftraggeber im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

Sofern und soweit die Leistungen und Tätigkeiten nicht in der Leistungsbeschreibung gemäß dem anwendbaren *Auftrag* enthalten sind oder der Auftraggeber nachweist, dass sie auf ein Verschulden des Auftragnehmer zurückzuführen sind, kann der Auftragnehmer für die nach Ziff. 2 anfallenden Tätigkeiten eine gesonderte Vergütung beanspruchen.

4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er feststellt, dass er oder ein Mitarbeiter bei der *Auftragsverarbeitung* gegen datenschutzrechtliche Vorschriften oder gegen Festlegungen aus der VAV oder dem anwendbaren *Auftrag* verstoßen hat/ haben, sofern und soweit deshalb die Gefahr besteht, dass *Auftraggeber-Daten* unrechtmäßig übermittelt oder auf sonstige Weise *Dritten* unrechtmäßig zur Kenntnis gelangt sind.

a) Der Auftragnehmer trägt dafür Sorge, dass der o.a. Kreis von Beteiligten zur Geheimhaltung gem. § 203 StGB verpflichtet wird. Dementsprechend wahrt der o.a. Kreis von Beteiligten in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht und den sonst anwendbaren rechtlichen Vorschriften fremde Geheimnisse, die von dem Auftraggeber zugänglich gemacht werden.

b) Der o.a. Kreis von Beteiligten verpflichtet sich, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Erfüllung eines *Auftrags* erforderlich ist.

c) Dem o.a. Kreis von Beteiligten ist bekannt, dass sich die Verschwiegenheitspflicht nicht nur auf fremde Geheimnisse erstreckt, sondern auf alle Tatsachen, die in Ausübung oder aus Anlass der Tätigkeit für den Auftraggeber, der einer beruflichen Verschwiegenheitsverpflichtung unterliegt, anvertraut oder bekannt werden. Hierzu gehört auch schon die Kenntnis, welche Mandate betreut werden.

d) Bei der Inanspruchnahme von Leistungen, die unmittelbar einem einzelnen Mandat oder einer einzelnen Person dienen, ist der Auftraggeber verpflichtet, die Einwilligung des Mandanten in die Zugänglichmachung von fremden Geheimnissen einzuholen.

e) Die vorstehend vereinbarte Pflicht zur Verschwiegenheit besteht nicht, soweit der Auftragnehmer auf Grund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggeberauftaggeber verpflichtet ist/wurde. Soweit dies im Einzelfall zulässig und möglich ist, wird der Auftragnehmer den Auftraggeber über die Pflicht zur Offenlegung möglichst vorab in Kenntnis setzen.

f) Dem Auftragnehmer ist die Rechtslage zu §§ 53a i.V.m. 53, 97 StPO, §§ 383 f ZPO bekannt (Mitwirkung an der beruflichen Tätigkeit eines Auftraggebers, der einer beruflichen Verschwiegenheitsverpflichtung unterliegt). Der o.a. Kreis von Beteiligten wird bei Gerichten und Behörden über Tatsachen, die mit der Tätigkeit bekannt werden, ohne vorherige Genehmigung des Auftraggeber nicht aussagen oder sonst Auskunft erteilen.

8. Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, arbeitstäglich (montags bis freitags ohne Feiertage am Standort des Auftragnehmer) zwischen 9:00 und 18:00 Uhr, auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmer, die Geschäftsräume des Auftragnehmer in denen *Auftraggeber-Daten verarbeitet* werden, zu betreten, um sich im gesetzlichen Rahmen von der Einhaltung der *TOM* und der Ordnungsgemäßheit der *Verarbeitung* zu überzeugen sowie die mit den *TOM* und der Ordnungsgemäßheit der *Verarbeitung* in Zusammenhang stehenden Unterlagen einzusehen (Kontrolle).

Sofern nicht anderweitig vereinbart, erfolgt eine Kontrolle durch den beruflich oder gesetzlich bzw. nach Maßgabe von Ziffer VI.4 zur Verschwiegenheit verpflichteten *DSB* des Auftraggeber.

Der Auftragnehmer gewährt dem Auftraggeber bzw. dessen *DSB* oder Prüfer die zur Durchführung der Kontrolle erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte. Eine Vor-Ort-Kontrolle ist grundsätzlich als Stichprobenkontrolle der für die Durchführung der *Auftragsverarbeitung* relevanten Bereiche auszugestalten.

Der Auftragnehmer ist – nach eigenem Ermessen, jedoch unter Berücksichtigung bestehender gesetzlicher Verpflichtungen des Auftraggeber – berechtigt, im Rahmen von Prüfungen und Kontrollen solche Informationen nicht zu offenbaren, die Betriebsgeheimnisse des Auftragnehmers enthalten (z.B. Informationen zu Kosten, Qualitätsprüfungs- und Vertrags-Managementberichte) oder durch deren Offenbarung der Auftragnehmer gegen gesetzliche oder Verpflichtungen aus Verträgen mit *Dritten* (z.B. Daten anderer Kun- den) verstoßen würde.

Der Auftraggeber hat den Auftragnehmer rechtzeitig - i.d.R. mindestens vier (4) Wochen vorher - über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände in Textform zu informieren und den Prüfungsumfang im Vorhinein zu dokumentieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen lassen, sofern nicht im *Auftrag* weitere Kontrollen vereinbart sind. Hiervon unbenommen ist das Recht des Auftraggeber, weitere Kontrollen durchzuführen, wenn er Kenntnis von sicherheitsrelevanten Vorgängen mit möglichen Auswirkungen auf *Auftraggeber-Daten* erlangt.

Beauftragt der Auftraggeber seinen *DSB* oder einen externen Prüfer mit der Durchführung der Kontrolle, hat der Auftraggeber den *DSB* bzw. Prüfer schriftlich ebenso zu verpflichten, wie der Auftraggeber selbst aufgrund von dieser Ziffer VIII. gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Prüfer auf Verschwiegenheit und Geheimhal- tung zu verpflichten. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen unverzüglich vorzulegen.

Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der *TOM* an- statt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, externe Datenschutz-Auditoren oder Qualitäts- Auditoren); oder durch eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutz-Auditoren erbracht werden, wenn die entsprechenden Dokumente es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der *TOM* zu überzeugen.

9. Unterauftragnehmer

Der Auftraggeber erteilt die Genehmigung, die für den Einsatz beim Auftraggeber vorgesehenen Unterauftragnehmer in Anspruch zu nehmen. Die jeweils aktuell im Bereich des Auftraggeber eingesetzten *Unterauftragnehmer* mit den für sie jeweils einschlägigen Arbeitsbereichen/ Tätigkeiten kann der Auftraggeber dort einsehen und diese jeweilige Aufstellung auf Wunsch ausdrucken. Der Auftraggeber speichert diese Aufstellung ab bzw. druckt sie aus; die Aufstellung ist Bestandteil dieser *VAV*.

Den dort jeweils genannten *Unterauftragnehmer* sind die datenschutzrechtlichen Pflichten aus dieser VAV ebenfalls auferlegt, sofern zwischen dem Auftraggeber und dem Auftragnehmer eine Vereinbarung nach Maßgabe von **Anlage 2** besteht, unter Berücksichtigung der dort etwa getroffenen zusätzlichen Maßgaben (vgl. Ziff. 3).

Der Auftraggeber wird informiert, wenn eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung der *Unterauftragnehmer* oder eine sonstige Änderung im Bereich der *Unterauftragnehmer* beabsichtigt ist. Die beabsichtigten Änderungen werden dem Auftraggeber in Textform mitgeteilt. Der Auftraggeber kann Einspruch gegen die beabsichtigte Änderung innerhalb von 4 (vier) Wochen nach Zugang der Information über die Änderung erheben.

Ein Einspruch nach Ziff. 3 bedarf eines wichtigen Grundes.

Im Fall des wirksamen Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern ihm die Erbringung der Leistung ohne die beabsichtigte Änderung nicht möglich oder nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb von 4 (vier) Wochen nach Zugang des Einspruchs kündigen.

Nicht zu den *Unterauftragnehmer* bzw. zu deren Leistungen hierzu gehören i.d.R. Nebenleistungen, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen. Zur Gewährleistung des Datenschutzes und der Datensicherheit der *Auftraggeber-Daten* sind vonseiten des Auftragnehmer auch bei solchen ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

10. Rechte der betroffenen Personen

Betroffene Personen können grundsätzlich ihre Rechte, insbes. solche gemäß Kapitel III der DS-GVO, nur gegenüber dem Auftraggeber als *Verantwortlichem* geltend machen. Wendet sich eine *betroffene Person* unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung, Löschung oder Einschränkung der *Verarbeitung* ihrer *personenbezogenen Daten*, wird dieses Ersuchen unverzüglich an den Auftraggeber weitergeleitet, soweit nicht ein Fall von Ziff. VI. 1. k) vorliegt.

Der Auftragnehmer unterstützt unter Berücksichtigung der Art der *Verarbeitung* und der ihm zur Verfügung stehenden Informationen den Auftraggeber bei der Einhaltung seiner Pflichten nach Kapitel III. DS-GVO gegenüber der betroffenen Person. Der Auftragnehmer wird es dem Auftraggeber durch entsprechende Maßnahmen nach jeweiliger Leistungsbeschreibung ermöglichen, *Auftraggeber- Daten* zu berichtigen, zu löschen oder die *Verarbeitung* einzuschränken oder auf dokumentiertes Verlangen des Auftraggeber hin die Berichtigung, Einschränkung der *Verarbeitung* oder Löschung vornehmen, wenn und soweit das dem Auftraggeber selbst technisch oder fachlich nicht möglich ist oder er dies gesondert beauftragt.

Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene gesonderte Vergütung vom Auftraggeber zu verlangen, sofern nicht ein Fall von Ziff. V. 1. k) vorliegt und diese Leistungen in der Leistungsbeschreibung oder anderweitig im *Auftrag* bepreist sind.

11. Rückgabe und Löschung von -Daten

Nach Abschluss der Erbringung der Leistungen zur *Verarbeitung* gemäß dem anwendbaren *Auftrag* führt der Auftragnehmer nach Wahl des Auftraggeber und nach Abstimmung der Vertragspartner eine der folgenden Tätigkeiten aus:

Er löscht alle nicht mehr erforderlichen *Auftraggeber-Daten*.

Er gibt diese in einem gängigen, im Zweifel in dem für die Verarbeitung der *Auftraggeber-Daten* verwendeten Format dem Auftraggeber zurück.

Er gibt diese in einem gängigen, im Zweifel dem für die Verarbeitung der *Auftraggeber-Daten* verwendeten Format an einen nachfolgenden Auftragsverarbeiter oder Dritten heraus (gem. Art. 20 Abs. 2 DS- GVO und bei Vorliegen der Voraussetzungen des Art. 20 DS- GVO).

Vorbehaltlich abweichender Vereinbarung werden unbeschadet der Regelung in Ziff. 1, die sich auf den Abschluss der jeweiligen Verarbeitungstätigkeit bezieht, jedenfalls bei Vertragsende die *Auftraggeber*-Daten auf einem vom Auftraggeber zuvor bereitgestellten Datenträger in dem für die Verarbeitung der *Auftraggeber-Daten* verwendeten Format an diesen übergeben und etwa beim Auftragnehmer vorhandene Kopien nach Maßgabe von Ziff. 1 gelöscht. Der Auftragnehmer wird ansonsten die Löschung innerhalb von neunzig (90) Tagen vornehmen.

Die Verpflichtung zur Löschung bzw. Übergabe nach den vorstehenden Absätzen gilt, sofern nicht Art. 17 Abs. 3 DSGVO greift, nach dem Recht der Europäischen Union oder nach deutschem Recht eine Verpflichtung zur Speicherung der *Auftraggeber-Daten* besteht oder sich aus dem *Auftrag* etwas anderes ergibt.

Der Aufwand für die Herstellung des Datenabzugs, sowie, falls gewünscht, die zusätzlichen Kurier- bzw. Transportkosten und ggfs. die Kosten eines Datenträgers, werden dem Auftraggeber gesondert in Rechnung gestellt.

Tätigkeiten zur Außerbetriebnahme, Datenübergabe bzw. Löschung erfolgen innerhalb der abgestimmten Zeiten, vorbehaltlich gesonderter Vereinbarung innerhalb der allgemeinen Arbeitszeiten der in Deutschland gelegenen Zentrale des Auftragnehmer.

Sofern ein *Auftrag* aus wichtigem Grund ganz oder teilweise fristlos oder sonst vorzeitig gekündigt oder auf andere Weise mit einer Frist von weniger als einer (1) Woche vorzeitig beendet wird, erhält der Auftraggeber die Gelegenheit, die von der (Teil-) Kündigung bzw. Beendigung betroffenen *Auftraggeber-Daten* innerhalb einer Frist von vier (4) Wochen nach rechtlicher Beendigung auf sich oder auf einen von ihm bestimmten Dritten nach Maßgabe von Ziff. 1 überzuleiten. Bewirkt der Auftraggeber eine Überleitung der *Auftraggeber-Daten* nicht innerhalb der o.a. Frist, d.h., nimmt er eine bestehende technische Möglichkeit der Überleitung innerhalb der Frist nicht wahr, ist der Auftragnehmer berechtigt, die *Auftraggeber-Daten* zu löschen.

Sofern Leistung gemäß dem *Auftrag* eine Datenaufbewahrung ist, z.B. eine Archivierung, insbesondere über die Laufzeit einer Verarbeitungstätigkeit hinaus werden diese *Auftraggeber-Daten* erst nach Ablauf der vereinbarten Archivierungszeit gelöscht. Wünscht der Auftraggeber eine relativ dazu vorzeitige Löschung, unterbreitet ihm der Auftragnehmer ein Angebot für die Vornahme der Löschungstätigkeit.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen *Auftragsverarbeitung* dienen, bewahrt der Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus auf.

Sofern und soweit sich unter Anwendung der vorstehenden Regelungen auch nach der rechtlichen Beendigung bzw. Teilbeendigung eines *Auftrages* noch von der Beendigung betroffene *Auftraggeber-Daten* auf Systemen des Auftragnehmers befinden, z.B. in Archiven, gelten die Vorschriften der VAV weiter.

12. Haftung

Für die Haftung gelten die Regelungen zur Haftung aus dem *Auftrag* entsprechend.

Sofern der Auftraggeber aus der DS-GVO oder aus anderen datenschutzrechtlichen Vorschriften, insbesondere gegenüber der *betroffenen Person* oder einer Aufsichtsbehörde, verpflichtet ist, ein DSGVO-konformes Verhalten nachzuweisen, gilt diese Beweislastverteilung auch im Innenverhältnis zum Auftragnehmer.

Die datenschutzrechtliche Verantwortung für die *Auftragsverarbeitung* verbleibt in dem gesetzlichen Rahmen beim Auftraggeber, d.h., soweit nicht datenschutzrechtliche Vorschriften Verpflichtungen für den Auftragnehmer einer *Auftragsverarbeitung* begründen und der Auftragnehmer diese Verpflichtungen nicht mindestens fahrlässig verletzt.

Soweit der Auftraggeber besonderen berufsrechtlichen Vorschriften unterliegt, haftet der Auftraggeber für deren Einhaltung.

13. Gültigkeit

Die VAV tritt nach Bestätigung durch den Auftraggeber in Kraft.

Die VAV löst eine ggfs. bestehende Vereinbarung zur Auftragsdatenverarbeitung nach § 11 BDSG der Vertragspartner nahtlos ab. Die Vertragspartner sind sich darüber einig, dass zwischen der VAV und einer etwa bestehenden bisherigen Vereinbarung zeitlich keine Lücke mit Blick auf die *Auftragsverarbeitung* bzw. Auftragsdatenverarbeitung besteht.

Etwa aus dem Zeitraum der Geltung der abgelösten Vereinbarung noch offene Ansprüche, z.B. auf Schadensersatz, werden nach der abgelösten Vereinbarung behandelt. Alle datenschutzrechtlich relevanten Ereignisse, die ab dem Inkrafttreten der VAV stattfinden, wer- den unter der VAV behandelt.

Laufzeit und Kündigung der VAV richten sich im Übrigen nach den Bestimmungen zur Laufzeit und Kündigung der von der VAV erfassten *Aufträge*. Eine auf Beendigung eines einzelnen *Auftrags* gerichtete wirksame Erklärung, gleich wann und aus welchem Grund, bewirkt ohne gesonderte Erklärung auch eine Kündigung der VAV auf denselben Zeitpunkt, bezogen jedoch nur auf den jeweils gekündigten *Auf- trag*. Eine Beendigung der VAV im Ganzen erfolgt vorbehaltlich abweichender Regelungen in Ziff. X insoweit nur mit der Beendigung des zeitlich letzten *Auftrages*. Eine isolierte Kündigung der VAV ist ausgeschlossen.

14. Verhältnis zum Auftrag

Soweit im Auftrag keine Sonderregelungen enthalten sind, gilt die VAV.

Im Fall von Widersprüchen zwischen der VAV einerseits und Regelungen aus sonstigen Vereinbarungen der Vertragspartner, insbesondere aus einem *Auftrag* andererseits, gehen die Regelungen aus dem Auftrag immer vor.

15. Schlussbestimmungen

Mündliche Nebenabreden werden nicht Vertragsbestandteil. Änderungen und Ergänzungen bedürfen der Textform (§ 126b BGB).

Auf das Rechtsverhältnis der Vertragspartner findet ausschließlich das Recht der Bundesrepublik Deutschland unter Ausschluss des UN- Kaufrechts und des Kollisionsrechts Anwendung.

Ausschließlicher, auch internationaler Gerichtsstand für alle sich aus dieser Vereinbarung unmittelbar oder mittelbar ergebenden Streitigkeiten ist das Landgericht am Sitz des Auftragnehmers. Diese Gerichtsstandsvereinbarung findet keine Anwendung, wenn die Streitigkeit andere als vermögensrechtliche Ansprüche betrifft oder für die Streitigkeit bereits nach den gesetzlichen Bestimmungen ein ausschließlicher Gerichtsstand begründet wird.

Sollte eine der Bestimmungen der VAV oder eine mit Bezug hierauf geschlossene weitere Vereinbarung, gleich wann und aus welchem Grund, unwirksam sein oder werden, oder die VAV eine nach übereinstimmender Auffassung der Vertragspartner regelungsbedürftige Lücke enthalten, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Vertragspartner werden in einem solchen Fall versuchen, die unwirksame oder lückenhafte Bestimmung durch eine neue Bestimmung zu ersetzen, die der unwirksamen oder lückenhaften Bestimmung nach dem Willen der Vertragspartner im Zeitpunkt der Unterzeichnung dieser Vereinbarung wirtschaftlich am Nächsten kommt. Bis zu einer solchen Ersetzung gelten anstelle der unwirksamen oder lückenhaften Bestimmung die gesetzlichen Regelungen.