Auftragsverarbeitung

Vereinbarung über die Auftragsverarbeitung personenbezogener Daten

zwischen den Lizenznehmern/Lizenznehmerinnen der Software AVP professional als Verantwortliche für die Verarbeitung personenbezogener Daten
- im Folgenden: Auftraggeber -

und der

AVP professional Software GmbH
Kurfürstendamm 56
10707 Berlin
vertreten durch:
Ralf Schäfer (Geschäftsführer) und Dr. Ulrich Steinmetzler, LL.M. (Geschäftsführer)
- im Folgenden: Auftragnehmer -

1. Einleitung, Geltungsbereich, Definitionen

1.1 Dieser Vertrag regelt die Rechte und Pflichten von Aufraggeber und Auftragnehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

1.2 Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

1.3 In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung (im Folgenden DSGVO) zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand, Dauer, Art und Zweck der Verarbeitung

2.1 Der Auftragnehmer verarbeitet auf Grundlage des geschlossenen Software-Lizenzvertrages personenbezogene Daten im Auftrag des Auftraggebers. Für die Verarbeitung der Daten hostet der Auftragnehmer die beiden Softwaremodule AVP finance planner und AVP finance tools in der Region Frankfurt/Main auf einer Serverlandschaft des Cloud- und Hosting Serviceunternehmens Amazon Web Services. Bei der Durchführung von Online-Meetings und Online-Webinaren nutzt der Auftragnehmer den Dienstleister GoTo Technologies Ireland Unlimited Company.

2.2 Der Vertrag wird auf unbestimmte Zeit geschlossen und endet mit Auftragserledigung, respektive mit Beendigung des zugrundliegenden Software-Lizenzvertrages.

2.3 Es werden je nach Eingabe folgende personenbezogene Daten verarbeitet:

Für die Berater(innen) als Lizenznehmer, die hiervon betroffen sind:

Art der Daten: Personenstammdaten (Registrierungsdaten für Benutzer der AVP-Webseiten wie Vor- & Nachname sowie Email-Adresse) / Vertragsstammdaten (Vertragslaufzeit, Software-Edition, Lizenzgebühren, Vertragsabrechnungs- & Zahlungsdaten etc.) / Kommunikationsdaten (nach freiwilliger Eingaben der Lizenznehmer(innen) z. B. Büro-Adresse, sonstige Adresse(n) & anderweitige Kontaktmöglichkeiten, z. B. Telefon-, Faxnummern & Email-Adressen etc.) / sonstige freiwillige Angaben (Berufsbezeichnung, Titel, Vermittlernummern, Firma, Unternehmen etc.);

Für die Mandantinnen/Mandanten, Kundinnen/Kunden, Interessenten etc. der Lizenznehmer(innen), die hiervon betroffen sind: Personenstammdaten (z. B. Vor- & Nachname, Geburtstag (Alter), Geschlecht, Kinder, familiärer, beruflicher & sozialversicherungsrechtlicher Status etc.) / Vertragsstammdaten (z. B. Finanzstatus wie Geldanlagen, Immobilien, Versicherungen, unternehmerische Beteiligungen, Investmentfonds, Darlehen, Sachwertefonds etc. / sonstige Angaben wie Absicherungs- & Versicherungsbedarf bzw. entsprechende Wünsche, finanzielle Ziele, berufliche Pläne etc.;

Für Webinarteilnehmer /-teilnehmerinnen, die hiervon betroffen sind:

Art der Daten: Personenstammdaten (Vor- und Nachname sowie Email-Adresse) / sonstige freiwillige Angaben (ID zum Weiterbildungskonto gut beraten).

2.4 Die Verarbeitung ist folgender Art: Erheben, Erfassen, Ordnen, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Verbreiten, Bereit stellen, Abgleichen, Verknüpfen, Einschränken, Löschen und Vernichten von Daten.

2.5 Die Daten werden verarbeitet, um den aktuellen Finanz- und Versicherungsstatus der Mandantinnen und Mandanten der Lizenznehmer darzustellen sowie anhand des genannten und gewünschten Versicherungs- und Absicherungsbedarfs sowie der genannten finanziellen Ziele die hierfür erforderlichen Maßnahmen berechnen zu können.

2.6 Die im Rahmen des Auftrags verarbeiteten Daten wird der Auftragnehmer selbst nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach schriftlicher Weisung des Auftraggebers berichtigen, löschen oder sperren.

3. Rechte und Pflichten des Auftraggebers

3.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung (Datenerhebung, -verarbeitung und -nutzung) sowie für die Wahrung der Rechte von Betroffenen ist der Auftraggeber verantwortlich.

3.2 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

3.3 Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte zu kontrollieren. 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. Für die Ermöglichung der Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

3.4 Der Umgang mit den Daten des Auftragsgebers durch den Auftragnehmer erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dessen Weisungen. Weisungen des Auftraggebers, die Art, Umfang und Verfahren der Datenverarbeitung durch den Auftragnehmer betreffen, sind von diesem mindestens in Textform (z. B. per Email) dokumentiert zu erteilen. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

4. Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen. Er verwendet die Daten für keine anderen Zwecke, insbesondere nicht für eigene Zwecke. Er ist nicht berechtigt, die Daten an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftragsgebers nicht erstellt. Ausgenommen hiervon sind Sicherungskopien, soweit sie zur Gewährleistung einer vertragsgemäßen Datenverarbeitung oder im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragsnehmer darf Daten darüber hinaus dann verwenden, wenn er gesetzlich zu einer bestimmten Verarbeitung verpflichtet ist. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen Zwecke.

4.2 Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.3 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung personenbezogener Daten die Vertraulichkeit streng zu wahren.

4.4 Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.5 Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden und dass er bzgl. Auswahl und Anleitung dieser Personen entsprechende datenschutzrechtliche Vorschriften einhält.

4.6 Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung

zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind dem Auftraggeber auf Anforderung zuzuleiten.

4.7 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 in dieser Vereinbarung geregelte Verarbeitung im Auftrag betroffen ist.

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

4.9 Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber mit. Derzeit ist Herr Carsten Kirschner, Corussoft GmbH, Kurfürstendamm 56, 10707 Berlin, Tel.: 030 / 8891 309-40 zum Datenschutzbeauftragten ernannt.

4.10 Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR.

5. Technische und organisatorische Maßnahmen

5.1 Der Auftragnehmer verpflichtet sich zur Umsetzung und Einhaltung der in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen und gewährleistet, dass diese unter Berücksichtigung der Anforderungen des Art. 32 DSGVO festgelegt wurden. Der Auftragnehmer legt auf schriftliche Anforderung des Auftragsgebers die näheren Umstände der Festlegung offen, soweit hierdurch keine vorrangigen Interessen, insbesondere Geheimhaltungsinteressen des Auftragnehmers betroffen sind.

5.2 Der Auftraggeber weist gesondert darauf hin, wenn besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO verarbeitet werden sollen oder sich aus anderen Gründen Besonderheiten bei der Beurteilung der Datenverarbeitung ergeben (z. B. hinsichtlich der Schwere eines Risikos für die Rechte und Freiheiten der betroffenen Personen etc.).

5.3 Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

5.4 Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

5.5 Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.6 Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.7 Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

6. Unterauftragsverhältnisse

6.1 Die Beauftragung von Subunternehmern seitens des Auftragnehmers ist nur möglich, wenn dem Subunternehmer vertraglich mindestens jene Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftragnehmer hat sicherzustellen, dass technische und organisatorische Maßnahmen entsprechend dieser Vereinbarung im Unterauftragsverhältnis umgesetzt werden und dass der Auftraggeber Kontroll- und Überprüfungsrechte im Umfang dieser Vereinbarung auch beim Subunternehmer wahrnehmen kann. Der Auftraggeber hat das Recht, von dem Auftragnehmer auf Anforderung in Textform Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrechtlichen Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsichtnahme in die relevanten Vertragsunterlagen, zu erhalten.

6.2 Der Auftraggeber erteilt seine allgemeine Zustimmung zur Einschaltung von Subunternehmern bei der Verarbeitung und/oder Nutzung personenbezogener Daten. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Einschaltung eines Subunternehmers und gibt dem Auftraggeber die Möglichkeit zum Widerspruch innerhalb einer Frist von 14 Tagen ab der Mitteilung.

6.3 Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

6.4 Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

6.5 Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat.

6.6 Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in diesem Vertrag genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche

konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

6.7 Zurzeit sind die in der Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Mit der Akzeptanz dieser Vereinbarung stimmt der Auftraggeber der Einbeziehung dieser Subunternehmer zu.

6.8 Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

7. Mitwirkung bei Beantwortung der Betroffenenrechte (Berichtigung, Sperrung und Löschung von Daten)

7.1 Die Wahrung der Betroffenenrechte gem. Art. 12 – 22 DSGVO obliegt der alleinigen Verantwortung des Auftraggebers. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte oder gegenüber dem Auftragnehmer der Datenverarbeitung widerspricht oder in Fällen von Profiling seinen eigenen Standpunkt mitteilt, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber zur Entscheidung weiterleiten. Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Dies gilt nicht bei einer entsprechenden gesetzlichen Verpflichtung. Auskünfte an den Betroffenen oder an Dritte darf der Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers erteilen.

7.2 Der Auftragnehmer ist im Rahmen der Mitwirkung an der Erfüllung der Informationspflichten gem. Art. 12 – 14 DSGVO nur zur Mitwirkung verpflichtet, soweit die Informationen ausschließlich ihm zugänglich sind und diese im Rahmen der sonstigen Pflichten dieses Vertrages nicht bereits übermittelt wurden.

7.3 Der Auftragnehmer ist lediglich verpflichtet, personenbezogene Daten an den Auftraggeber in dem Format herauszugeben, in dem er diese von ihm zur Verarbeitung im Rahmen dieses Vertrages erhalten hat. Sowohl die Herausgabe in einem sonstigen strukturierten, gängigen und maschinenlesbaren Format als auch die Herausgabe direkt an den Betroffenen oder an einen von diesem bestimmten weiteren Verantwortlichen sind nur auf Grundlage einer ausdrücklichen Weisung und bei Übernahme der hierdurch entstehenden zusätzlichen Kosten geschuldet.

8. Mitteilungspflichten

8.1 Der Auftragnehmer teilt dem Auftraggeber ihm bekannt gewordene Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung hat mindestens die Angaben nach Art. 33 Abs. 3 DSGVO zu enthalten. Die Bewertung des mit dieser Verletzung verbundenen Risikos obliegt alleine dem Auftraggeber. Der

Auftragnehmer wirkt hieran nur durch die Meldung der Verletzung sowie die Bereitstellung von Informationen nach dieser Vereinbarung mit.

8.2 Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

8.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur hier geregelten Auftragsverarbeitung aufweisen. Sollen Empfehlungen der Aufsichtsbehörde gemäß Art. 36 Abs. 2 DSGVO Grundlage der Datenverarbeitung nach dieser Vereinbarung werden, so hat der Auftraggeber diese durch ausdrückliche Weisung zu bestätigen. Dies gilt insbesondere auch für Empfehlungen, die die Aufsichtsbehörde direkt gegenüber dem Auftragnehmer macht. Der Auftragnehmer informiert den Auftraggeber über ihm unmittelbar mitgeteilte Empfehlungen und Fristverlängerungen der Aufsichtsbehörde gem. Art. 36 Abs. 2 DSGVO. Zur Umsetzung zusätzlicher technischer und organisatorischer Maßnahmen zu den gem. Ziff. 5.1. getroffenen ist der Auftragnehmer nur gegen Übernahme der hierdurch entstehenden zusätzlichen Kosten durch den Auftraggeber verpflichtet.

8.4 Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

8.5 Der Auftragnehmer ist zur Mitwirkung im Rahmen der Datenschutz-Folgeabschätzung nur soweit verpflichtet, als der Auftraggeber für die vorzunehmende Bewertung des Risikos der Datenverarbeitung neben den von dem Auftragnehmer nach dieser Vereinbarung zur Verfügung gestellten Informationen noch weitere Auskünfte benötigt. Insbesondere ist der Auftragnehmer nicht verpflichtet, eine Abschätzung gem. Art. 35 DSGVO für eigene Verarbeitungsprozesse vorzunehmen.

9. Weisungen

9.1 Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein Weisungsrecht vor.

9.2 Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen befugten Personen.

9.3 Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter mitzuteilen.

9.4 Der Auftragnehmer hat dem Auftraggeber umgehend zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

9.5 Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

10. Beendigung des Auftrags

10.1 Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Der Auftraggeber teilt dem Auftragnehmer rechtzeitig mit, sofern Daten für die auftragsgemäße Verarbeitung nicht weiter benötigt werden. Im Zweifel ist die Verarbeitungsleistung mit Vertragsende abgeschlossen. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399.

10.2 Der Auftragnehmer ist verpflichtet, die von einer Vertragsbeendigung betroffenen Datenbestände für einen Zeitraum von 30 Tagen nach Auftragsende aufzubewahren. Der Auftraggeber ist berechtigt, jederzeit bis zum Ablauf dieser Frist die Herausgabe oder die Löschung der gespeicherten Datenbestände zu verlangen.

10.3 Erteilt der Auftragnehmer eine verbindliche Löschungsbestätigung in Textform, so ist der Auftragnehmer berechtigt und verpflichtet, auch vor Ablauf der Aufbewahrungsfrist gem. Ziff. 10.2 die Datenlöschung innerhalb von einer Woche nach Zugang der Bestätigungserklärung durchzuführen. Hiervon ausgenommen sind lediglich Daten, hinsichtlich derer der Auftragnehmer gesetzlich zur Aufbewahrung verpflichtet ist.

10.4 Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

10.5 Der Auftragnehmer hat auf Anforderung durch den Auftraggeber den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber vorzulegen.

10.6 Dokumentation, die dem Nachweis der auftrags- und vertragsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Der Auftragnehmer kann diese zu seiner Entlastung dem Auftragsgeber nach Vertragsende übergeben.

11. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht. Ausgenommen hiervon ist ein möglicher Vergütungsanspruch gem. Ziff. 3.3 und Ziff. 8.3.

12. Haftung

12.1 Der Auftragnehmer haftet dem Auftraggeber nur für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

12.2 Soweit eine Haftung des Auftragnehmers ganz oder teilweise ausgeschlossen ist, stellt der Auftraggeber den Auftragnehmer von allen Ansprüchen frei, die Dritte wegen der Datenverarbeitung im Auftrag des Auftragsgebers gegen den Auftragnehmer erheben. Das gilt insbesondere auch, soweit eine Inanspruchnahme als Gesamtschuldner den auf den Auftragnehmer entfallenden Verschuldensanteil summenmäßig übersteigt. Der Auftraggeber ist verpflichtet, den Auftragnehmer in angemessener Art und Weise bei dessen Verteidigung gegenüber den von Dritten erhobenen Ansprüchen zu unterstützen, dem Auftragnehmer alle geeigneten Beweismittel zugänglich zu machen sowie dem Auftragnehmer die Vorlage aller zur Entlastung geeigneter Informationen zu gestatten.

13. Sonderkündigungsrecht

13.1 Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

13.2 Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

13.3 Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

14. Sonstiges

14.1 Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

14.2 Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

14.3 Für Nebenabreden ist die Schriftform erforderlich.

14.4 Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

14.5 Es gilt das Recht der Bundesrepublik Deutschland.

14.6 Für alle Streitigkeiten im Zusammenhang mit dieser Vereinbarung wird der Sitz des Auftragnehmers als ausschließlicher Gerichtsstand vereinbart. Der Auftragnehmer bleibt berechtigt, den Auftraggeber an dessen allgemeinen Gerichtsstand zu verklagen.

Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen beschrieben, die die AVP professional Software GmbH für Ihre Dienstleistungen getroffen hat und künftig zu treffen hat, um die Erfordernisse datenschutzrechtlicher Regelungen zu gewährleisten. Ziel ist der Schutz insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1. Verschlüsselung und Pseudonymisierung personenbezogener Daten

Gewährleistung, dass personenbezogene Daten im System nur in einer Weise gespeichert werden, die Dritten die Zuordnung zum Betroffenen nicht ermöglicht;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z. B.: keine Pseudonymisierung personenbezogener Daten innerhalb der verschlüsselten Datenbank (dies ist nicht sinnvoll wegen der unten genannten technischen Maßnahmen zur ausschließlich lizenzbezogenen Nutzung personenbezogener Daten, da ansonsten kein Einzelsupport durch Verwalter des AVP/AWS-Accounts geleistet werden kann) / keine Pseudynomisierung von übermittelten personenbezogenen Daten zu Test-, Analyse- und Beratungszwecken, jedoch Vernichtung der Daten nach Verwendung / ansonsten gilt: Gewährleistung der ausschließlich lizenzbezogenen Nutzung personenbezogener Daten durch technische Maßnahmen wie getrennte Server für AVP-Anwendung, AVP-Webseiten und AVP-Datenbank innerhalb einer VPC (Virtual Private Cloud) innerhalb der AWS-Serverlandschaften, AWS-Verschlüsselung des Datenbankservers, Nutzung von Berechtigungskonzepten für den Zugriff auf den AVP-Datenbankserver über den AVP-Applikationsserver durch Authentifizierung und Autorisierung durch AVP-Account und Passwörtern, Zuordnung der personenbezogenen Daten auf dem Datenbankserver nur an authentifizierte und autorisierte Lizenznehmer.

2. Vertraulichkeit und Integrität

2.1. Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte;

Verantwortlich hierfür ist: Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, Washington 98109-5210, Vereinigte Staaten, Rechenzentrum in Frankfurt am Main, europäischem Recht unterstehend;

Entsprechende Maßnahmen sind z. B.: architektonische Maßnahmen wie „physische“ Eintrittsbarrieren sowohl im Umkreis als auch zu den Gebäuden,

separate Gebäude und jeweils separate Serverräume mit getrennten Schließungen / technische Maßnahmen wie Sicherheitsschließanlagen zu den Gebäuden und Serverräumen, Zutrittskontrollsysteme (Code- und/oder Ausweisleser, Magnet- und/oder Chipkarten), Zwei-Faktor-Authentifizierung speziell autorisierter Mitarbeiter für Rechenzentrums-Etagen, Videoüberwachung, Einbrucherkennungssysteme, Alarmanlagen / organisatorische Maßnahmen wie Zugangskontrollen durch professionelles Sicherheitspersonal, Überwachung aller Mitarbeiter und Protokollierung aller Arbeiten auf Rechenzentrums-Etagen etc., siehe hierzu – sowie zu den anderen Punkten unten – bitte auch d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

2.2. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern;

Verantwortlich hierfür ist: Amazon Web Services;

Entsprechende Maßnahmen sind z. B.: architektonische Maßnahmen wie oben beschrieben / technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – modernste Netzwerk Firewall-Technologien (Anti-Viren-Software & Hardware-Schutz), Datenverkehrskontrolle durch AWS Security Groups, automatische Sperrmechanismen / organisatorische Maßnahmen wie oben beschrieben / für die Datenträgerkontrolle gilt: die relevanten Datenträger befinden sich ausschließlich innerhalb der AWS-Serverlandschaften, andere relevante Datenträger gibt es nicht;

Verantwortlich hierfür ist: AVP Professional Software GmbH, Kurfürstendamm 56, 10707 Berlin, HRB 150440, Deutschland, siehe www.avp-professional.de;

Entsprechende Maßnahmen sind z. B.: technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – 2-Wege-Authentifizerung für Verwalter des AVP/AWS-Accounts.

2.3. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten;

Verantwortlich hierfür ist: Amazon Web Services;

Entsprechende Maßnahmen sind z. B.: technische Maßnahmen wie oben beschrieben / organisatorische Maßnahmen wie oben beschrieben;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind: technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – Bestimmung der Sicherheitsstufen zur Passwortverwendung, Ermöglichung der Nutzung, Verwaltung, Löschung und Änderung der Zugangsdaten (Email-Adressen und Passwörter) zu den Softwareanwendungen ohne Kenntnis des Auftragnehmers und der Subunternehmer;

Verantwortlich hier ist: der Auftraggeber;

Entsprechende Maßnahmen sind z.B.: organisatorische Maßnahmen wie keine Verwendung von „einfachen“ Passwörtern (z. B. 12345678), keine Weitergabe von „sicheren“ Passwörtern an unbefugte Personen.

2.4. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z. B.: technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – ausschließliche SSL-Verschlüsselung aller Daten (Transport- und Inhaltsverschlüsselung aller Daten, die zwischen dem Browser des Auftraggebers und den Serverlandschaften von AWS in beide Richtungen versandt werden), zertifikatsbasierte Datenverschlüsselung zwischen den oben genannten AVP-Servern innerhalb der VPC.

2.5. Zugriffskontrolle (i.e.S.)

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z. B.: technische Maßnahmen wie oben beschrieben / organisatorische Maßnahmen wie Reduzierung der Anzahl der Verwalter des AVP/AWS-Accounts auf das „Notwendigste“;

Verantwortlich hierfür ist: der Auftraggeber;

Entsprechende Maßnahmen sind z. B.: organisatorische Maßnahmen wie Verwaltung von Benutzern der Nebenlizenzen sowie deren Zugangsdaten.

2.6. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z. B.: technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – Protokollierung und Benutzerkennung (Protokollierung des Auftragsgebers bei Eingabe und Änderung von Daten).

2.7. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z. B.: technische Maßnahmen wie oben beschrieben / ansonsten gilt: ein physischer Transport von Datenträgern findet nicht statt, entsprechende Sicherheitsmaßnahmen sind daher irrrelevant.

2.8. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z. B.: technische Maßnahmen wie oben beschrieben.

2.9. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können;

Verantwortlich hierfür ist: Amazon Web Services; siehe aws.amazon.com/de

Entsprechende Maßnahmen sind z. B.: architektonische Maßnahmen wie – zusätzlich zu den oben beschriebenen – Brandschutzmaßnahmen durch getrennte Gebäude- und Raumeinheiten / technische Maßnahme wie – zusätzlich zu den oben beschriebenen – automatisierte Löschanlagen, unterbrechungsfreie Stromversorgung durch Überspannungsschutz etc., Klimaanlage, zentrale Überwachungseinheit zur Kontrolle aller Betriebsparameter des Rechenzentrums mit Alarmierung.

2.10. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z. B.: organisatorische Maßnahmen wie eindeutige Vertragsgestaltung, Bestellung eines Datenschutzbeauftragten beim Auftragnehmer, Unterweisung aller Mitarbeiter des Auftragsnehmers und seiner Subunternehmer auf Wahrung des Datenschutzgeheimnisses, sorgfältige Auswahl der Subunternehmer.

3. Verfügbarkeit

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind;

Verantwortlich hierfür ist: Amazon Web Services;

Entsprechende Maßnahmen sind z. B.: architektonische Maßnahmen wie oben beschrieben / technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – AWS- Backup-Konzept und Backup-Verfahren;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z B.: technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – AVP Backup-Konzept und Backup-Verfahren.

4. Belastbarkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Verantwortlich hierfür ist: Amazon Web Services;

Entsprechende Maßnahmen sind z. B.: architektonische Maßnahmen wie oben beschrieben / technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – modernste Netzwerk Firewall-Technologien mit DDoS-Schutzmechanismen.

5. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Verantwortlich hierfür ist: Amazon Web Services;

Entsprechende Maßnahmen sind z. B.: technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – AWS- Backup-Konzept und Backup-Verfahren mit täglicher Sicherung aller relevanten Daten.

6. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene, personenbezogene Daten getrennt verarbeitet werden können;

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z. B.: technische Maßnahmen wie – zusätzlich zu den oben beschriebenen – Trennung der personenbezogenen Daten der Lizenznehmer und der personenbezogenen Daten der Mandantinnen/Mandanten, Kundinnen/Kunden, Interessenten etc. der Lizenznehmer(innen), Trennung von Produktsystemen und Testsystemen.

7. Überprüfung und Evaluierung

Darstellung des Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Verantwortlich hierfür ist: AVP Professional Software GmbH;

Entsprechende Maßnahmen sind z. B.: sorgfältige Auswahl der Subunternehmer.

Anlage 2 – Auftragnehmer und zugelassene Subdienstleister

Auftragnehmer im Einzelnen sind:

- AVP professional Software GmbH, Kurfürstendamm 56 in 10707 Berlin (Software-Dienstleister und Auftragnehmer),

- Corussoft GmbH, Kurfürstendamm 56 in 10707 Berlin (technischer Software-Dienstleister und Auftragnehmer),

- Amazon Web Services (Betreiber Rechenzentrum).

Stand: Mai 2018