Version 1.0 gültig ab 25.05.2018

Vertrag über die Auftragsverarbeitung personenbezogener Daten (im folgenden kurz VAv oder Vertrag)

Zwischen

dem **Kunden** (im Folgenden Kunde oder auch Auftraggeber genannt)

Und

der **TabTool GmbH** (im Folgenden Auftragnehmer genannt)

beide einzeln oder gemeinsam auch Partei oder Parteien genannt.

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

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

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung 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.

(4) Dieser Vertrag ergänzt den zwischen den Parteien geschlossenen Hauptvertrag, der mit dem Kauf einer Lizenz für die Nutzung von durch TabTool vertriebenen Anwendungen in Kraft tritt. Dies schließt gegebenenfalls vereinbarte kostenlose Testphasen ein.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen:

TabTool stellt dem Kunden eine Software zur Verfügung, in welcher der Kunde selber Daten verwalten kann. Hierbei können durch den Kunden auch personenbezogene Daten erhoben werden. Eine über die Funktionalitäten der Software hinausgehende Verarbeitung der durch den Kunden eingegebenen Daten findet nicht statt. Ein Zugriff auf die personenbezogenen Daten des Kunden durch Mitarbeiter von TabTool ist nicht vorgesehen, es sei denn der Kunde genehmigt dies explizit im Rahmen einer Support-Anfrage oder Wartungsarbeiten an der Software sind ohne den Zugriff nicht möglich. Im zweiten Fall wird TabTool den Kunden vor dem Beginn der Wartungsarbeiten informieren und so die Möglichkeit schaffen Datenschutzrechtliche Vorkehrungen mit dem Kunden abzustimmen.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag (im Folgenden „Hauptvertrag“).

2.2 Dauer

Die Verarbeitung beginnt mit dem Zustandekommen des Hauptvertrages zwischen den beiden Parteien. Der Hauptvertrag kommt automatisch mit der Registrierung für die Nutzung einer von TabTool vertriebenen Anwendung zustande, ihm liegen die AGB von TabTool zugrunde. Dieser VAv erlischt automatisch durch die Beendigung des Hauptvertrages, und zwar zu dem Zeitpunkt an dem alle unter diesen Vertrag fallenden Daten durch den Auftragnehmer gelöscht oder übergeben wurden. Nach dem Ende des Hauptvertrages werden die Daten durch den Auftragnehmer noch bis zu zwei Monaten weiter vorgehalten, um eine Reaktivierung des Hauptvertrages zu ermöglichen. Der Kunde kann jedoch eine sofortige Löschung sämtlicher Daten beantragen.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1 Art und Zweck der Verarbeitung

TabTool ist ein Werkzeug zur Dokumentation, Planung und Durchführung von (Projekt-)Arbeiten. Für den vorgenannten Zweck notwendige personenbezogene Daten werden in diesem Kontext erhoben,

erfasst, organisiert, geordnet, gespeichert, angepasst oder verändert, ausgelesen, abgefragt, verwendet, innerhalb des Systems miteinander oder mit anderen Daten verknüpft und gegebenenfalls über eine Schnittstelle in andere Software des Kunden übertragen.

3.2 Art der Daten und Kategorien der betroffenen Personen

In den Produkten von TabTool ist die folgende Verarbeitung von personenbezogenen Daten vorgesehen:

Es werden folgende Daten verarbeitet:

Kategorien betroffener Personen	**Art der Daten**	**Zweck der Datenverarbeitung**
TabTool-Benutzer	***Identifikationsdaten*** *Vor- und Nachname / Adressinformationen (Straße, Hausnummer, Stadt, PLZ) / Telefon / Handy / Fax / E-Mail-Adresse* ***Personaldaten*** *Mitarbeiterorganisationsinformationen (Telefon, Mobil, Fax, E-Mail) / Mitarbeiterstandortinformationen (Hausnummer, Straße, Stadt, PLZ) / Abteilung / Rolle* ***Individuelle Daten*** *Verkehrsdaten / Protokolldaten (Log-in / Log-off) / Passwörter / Verkehrsdaten Netzwerk / Systemdaten (Konfigurationsinformationen, Update-Informationen, Alarmmeldungen, wenn personenbeziehbar) / IP Konfigurationsinformation, Netzwerkidentifikationsinformationen, wenn personenbeziehbar)* ***Weitere Daten*** *Dem Kontakt zugeordnete Bilder, Notizen, Dokumente*	Zugang zur Anwendung Funktionalität der Anwendung
Kontaktpersonen des Kunden	***Identifikationsdaten*** *Vor- und Nachname / Adressinformationen (Straße, Hausnummer, Stadt, PLZ) / Telefon / Handy / Fax / E-Mail-Adresse* ***Personaldaten*** *Mitarbeiterorganisationsinformationen (Telefon, Mobil, Fax, E-Mail) / Mitarbeiterstandortinformationen*	Erfüllung des Zwecks im jeweiligen Produkt

	(Hausnummer, Straße, Stadt, PLZ) / Abteilung / Rolle ***Weitere Daten*** *Dem Kontakt zugeordnete Bilder, Notizen, Dokumente*	

Es ist keine Verarbeitung von Daten vorgesehen die unter den §9 der DSGVO fallen. Der Kunde hat dafür Sorge zu tragen, dass keine diesbezüglichen Informationen verarbeitet werden. Sollte ein berechtigtes Interesse des Kunden bestehen diese Daten zu verarbeiten muss hierüber mit TabTool eine gesonderte Vereinbarung getroffen werden.

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. 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, insbesondere nicht für eigene Zwecke.

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

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(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.

(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. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(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 vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(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 Verarbeitung im Auftrag betroffen ist.

(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 unverzüglich an den Auftraggeber weiterleiten.

(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 unverzüglich 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 unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

(11) Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.

5 Technische und organisatorische Maßnahmen

(1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

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

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

(5) 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.

(6) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

(7) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

(2) 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.

(3) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(4) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

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

(6) 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. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.

(7) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nicht möglich.

(8) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen.

(9) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

(10) Zurzeit sind die in 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. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(11) 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.

8 Rechte und Pflichten des Auftraggebers

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

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

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

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich 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.

(5) 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. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

   a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
   b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
   c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
   d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(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.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Der Auftragnehmer benennt die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3. Seitens des Auftragnehmers ist der Vertragshalter selbst weisungsbefugt, die Weisungsbefugnis kann schriftlich auf weitere Personen ausgeweitet werden.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

(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. 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. Hierbei gilt mindestens Schutzklasse 3.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den

Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der Auftragnehmer haftet dem Auftraggeber 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.

(4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

14 Sonderkündigungsrecht

(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.

(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.

(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.

(4) Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.

(5) Verstößt der Auftraggeber gegen die in diesem Vertrag genannten Verpflichtungen hat der Auftragnehmer ebenfalls ein außerordentlichen Kündigungsrecht. Dies gilt insbesondere für den Fall der Erfassung von personenbezogenen Daten durch den Auftraggeber die nicht explizit Teil in diesem Vertrag genannt werden (z.B. die Erfassung von Daten nach §9 DSGVO).

15 Sonstiges

(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.

(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.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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

Anlage 1 – technische und organisatorische Maßnahmen (Stand 25.05.2018)

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

(1) Zutrittskontrolle

a. Die Daten des Kunden liegen ausschließlich in einem zertifizierten Rechenzentrum eines vom Auftragnehmer beauftragten Hosters.

(2) Zugangskontrolle

a. Durch von uns bereitgestellte Sicherheitsmechanismen, wie ein persönliches Login und Passwort, eine persönliche Sicherheitsabfrage und dem IT-Zugriffsschutz, ermöglichen wir Ihnen die Nutzung des Systems durch Unbefugte zu verhindern. (Zugangskontrolle)

b.

(3) Zugriffskontrolle

a. Mitarbeiter des Auftragnehmers

   i. Ein Berechtigungskonzept regelt die Vergabe und den Entzug von Rechten.

   ii. Der Status des Berechtigungsmanagements wird regelmäßig im Datenschutzreport berichtet.

   iii. Veränderungen an den Berechtigungen werden revisionssicher dokumentiert.

   iv. Klare Verhaltensregeln für die Mitarbeiter stellen sicher, dass die DV-Ausstattung ausreichend gegen Fremdzugriff gesichert ist. Dies schließt die Grundsätze des „aufgeräumten Schreibtisches“ und des „leeren Bildschirms“ ein.

   v. Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren. Vor Durchführung der Prüfungs- und Wartungsarbeiten werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherungsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

   vi. Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfange - auch in zeitlicher Hinsicht - Gebrauch machen, als dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten unerlässlich notwendig ist.

vii. Der Auftragnehmer wird Daten auf Speichermedien, die er aufgrund von Prüfungs- oder Wartungsarbeiten im Rahmen eines Austauschs, einer Vertragsaufhebung oder zur Vernichtung erhält, dauerhaft löschen. Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragnehmer angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen.

viii. Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z.B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Zustimmung des Auftraggebers einholen. Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Zustimmung des Auftraggebers. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchen des Auftragnehmers verwendet werden, sofern die vorherige Zustimmung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB-Speichersticks, CDs, DVDs oder ähnliche Geräte) kopiert werden.

b. Nutzer auf Seite des Kunden

i. Unsere umfassende administrative Rechtevergabe für Gruppen und Benutzer reicht bis hin zum personenbezogenen Lese-, Bearbeitungs- und Schreibschutz von Modulen, Kontakten, Projekten oder auch Ordnern und Dokumenten. Somit können Sie detailliert einstellen, dass "Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können".

(4) Weitergabekontrolle

a. Alle Personen, die personenbezogene Daten verarbeiten oder mit ihnen in Berührung kommen könnten sind auf das Datengeheimnis verpflichtet.

b. Neue Mitarbeiter erhalten Informationen zum Datenschutz beim Umgang mit personenbezogenen Daten.

c. Physische Datenübergaben von Kundendaten sind nicht vorgesehen.

d. Personenbezogene Daten werden durch TabTool nicht weitergegeben.

e. Eine elektronische Weitergabe über Schnittstellen findet nur zwischen TabTool und den Zielsystemen des Kunden statt.

f. Die Übertragung von Daten zwischen verschiedenen Anwendungskomponenten erfolgt stets verschlüsselt, so dass während der Übertragung kein Zugriff durch dritte möglich ist.

g.

(5) Trennungskontrolle

a. Die Daten verschiedener Kunden sind bei TabTool vollständig voneinander getrennt. Die Daten sind wechselseitig nicht einsehbar.

b. Entwicklungs- und Testsysteme sind logisch klar von Produktivsystemen getrennt.

c. TabTool bietet dem Kunden die Möglichkeit zu verschiedenen Zwecken erhobene Daten voneinander getrennt zu speichern.

(6) Weitere Sicherungsmaßnahmen

a. Eine vollständige Eingabekontrolle und Historie der von Kunden und Ihren Nutzern eingegebenen Daten ermöglicht es, "dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind".

b. Ihre Daten sind gegen zufällige Zerstörung oder Verlust geschützt durch eine systeminterne Backup-Funktion von bis zu 30 Tagen sowie separate Backup-Server zur täglichen Datensicherung mit 7-tägiger Vorhaltedauer.

Anlage 2 – Zugelassene Subdienstleister

Double C GmbH, Im Sand 23, 25451 Quickborn

Überlassung von Mitarbeitern für die Weiterentwicklung und Betreuung von TabTool-Systemen.

Anlage 3 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Dirk Brockmeyer, TabTool GmbH

Ulf Stabe, TabTool GmbH