

AVV

Vereinbarung zur Auftragsverarbeitung

Nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen

dem Nutzer der Plattform GutachterBook als Verantwortlichem
(nachfolgend „Auftraggeber“)

und

GutachterBook – Faik-Salih Cansu & Sebastian Fröhlich GbR,
Unter den Eichen 103, 40625 Düsseldorf,
vertreten durch die Gesellschafter Faik-Salih Cansu und Sebastian Fröhlich,
als Auftragsverarbeiter
(nachfolgend „Auftragnehmer“)
(Auftraggeber und Auftragnehmer nachfolgend gemeinsam „Parteien“)

Inhalt

1.	Gegenstand, Geltungsbereich und Dauer der Verarbeitung	2
2.	Art und Zweck der Verarbeitung	2
3.	Art der personenbezogenen Daten und Kategorien betroffener Personen	2
4.	Verantwortlichkeit und Verarbeitung auf dokumentierte Weisungen	3
5.	Rechte des Auftraggebers, Pflichten des Auftragnehmers	3
6.	Pflichten des Auftraggebers	5
7.	Anfragen betroffener Personen	5
8.	Maßnahmen zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO	5
9.	Nachweis und Überprüfung	6
10.	Subunternehmer (weitere Auftragsverarbeiter)	6
11.	Löschung und Rückgabe von Daten	7
12.	Haftung und Schadensersatz	8
13.	Vertragslaufzeit, Änderungen, Sonstiges	8
Anhang 1	Leistungsbeschreibung, Datenkategorien und betroffene Personen	9
Anhang 2	Subunternehmer (weitere Auftragsverarbeiter)	11
Anhang 3	Technische und organisatorische Maßnahmen (TOM)	12
Anhang 4	Annahme und Unterzeichnung	15

1. Gegenstand, Geltungsbereich und Dauer der Verarbeitung

1.1 Gegenstand dieser Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß den Nutzungsbedingungen und der Leistungsbeschreibung der Plattform GutachterBook (nachfolgend „Hauptvertrag“), soweit eine Verarbeitung personenbezogener Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber als Verantwortlichen gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Hauptvertrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Hauptvertrag nicht ausdrücklich auf diese Vereinbarung verweist.

1.2 Der Auftragnehmer betreibt die unter gutachterbook.de erreichbare Online-Plattform GutachterBook (nachfolgend „Plattform“). Der Auftraggeber nutzt die Plattform zur Online-Terminvergabe für Kfz-Sachverständigenleistungen sowie zur Verwaltung seiner Kunden, Fahrzeuge, Schadensvorgänge, Termine und Gutachten. Die Leistungen sind in Anhang 1 beschrieben.

1.3 Nicht Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten, die der Auftragnehmer in eigener Verantwortung vornimmt. Dies betrifft insbesondere den Betrieb der öffentlich zugänglichen Website, die Verwaltung von Nutzerkonten, die Endkunden unmittelbar beim Auftragnehmer anlegen, die Suche und Auswahl eines Sachverständigenbüros durch Endkunden, bevor ein Termin bei dem Auftraggeber gebucht wird, sowie die Anbahnung, Durchführung und Abrechnung des Hauptvertrags. Für diese Verarbeitungen ist der Auftragnehmer selbst Verantwortlicher und erfüllt die Informationspflichten nach Art. 13 und 14 DSGVO in seiner Datenschutzerklärung. Sobald ein Endkunde einen Termin bei dem Auftraggeber bucht oder der Auftraggeber Daten einer Person in der Plattform erfasst, erfolgt die weitere Verarbeitung dieser Daten im Auftrag des Auftraggebers nach Maßgabe dieser Vereinbarung. Hiervon unberührt bleiben Verarbeitungsvorgänge, für die der Auftragnehmer aufgrund eines eigenen, von den Zwecken des Auftraggebers unabhängigen Zwecks selbst Verantwortlicher ist; solche Verarbeitungsvorgänge werden in der Datenschutzerklärung gesondert ausgewiesen.

1.4 Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrags. Findet eine Verarbeitung personenbezogener Daten des Auftraggebers nach dessen Beendigung noch statt, insbesondere während der Exportfrist nach Ziffer 11, gelten die Regelungen dieser Vereinbarung bis zum tatsächlichen Ende der Verarbeitung fort.

2. Art und Zweck der Verarbeitung

2.1 Die Art der Verarbeitung umfasst das Erheben, Erfassen, Speichern, Ordnen, Auslesen, Verändern, Übermitteln per E-Mail an die betroffene Person, Löschen und Anonymisieren personenbezogener Daten in einer Web-Anwendung mit zugehöriger Datenbank und Dateiablage.

2.2 Zwecke der Verarbeitung sind die Online-Terminvergabe für Kfz-Sachverständigenleistungen des Auftraggebers, die Verwaltung seiner Kunden- und Fahrzeugstammdaten, die Dokumentation von Fahrzeugschäden sowie die Erstellung, Ablage und Übermittlung von Gutachten (siehe hierzu auch Anhang 1).

3. Art der personenbezogenen Daten und Kategorien betroffener Personen

3.1 Gegenstand der Verarbeitung sind Stammdaten, Fahrzeugdaten, Schadensdaten, Vorgangsdaten, Notizen, Zugangsdaten sowie Nutzungs- und Verbindungsdaten. Die einzelnen Datenkategorien sind in Anhang 1 aufgeführt. Über die dort genannten Kategorien hinaus bestimmt der Auftraggeber die Art der verarbeiteten Daten durch die Nutzung der Plattform und die von ihm erfassten Inhalte.

3.2 Kategorien betroffener Personen sind Kunden des Auftraggebers (Fahrzeughalter, Auftraggeber von Gutachten), Interessenten, die über die Plattform einen Termin bei dem Auftraggeber buchen, Beschäftigte des Auftraggebers als Nutzer der Plattform sowie weitere Personen, deren Daten der Auftraggeber im Rahmen eines Schadensvorgangs erfasst (z. B. weitere Unfallbeteiligte, Fahrzeughalter, Versicherungsnehmer).

3.3 Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand dieser Vereinbarung. Die Plattform sieht hierfür keine Felder vor. Der Auftraggeber stellt sicher, dass er insbesondere in Freitextfeldern keine Gesundheitsdaten – etwa Angaben zu Personenschäden – erfasst. Werden solche Angaben dennoch erfasst, bleibt der Auftraggeber hierfür Verantwortlicher; er entfernt sie unverzüglich, sobald

er davon Kenntnis erlangt, und der Auftragnehmer unterstützt ihn dabei auf Weisung. Stellt der Auftragnehmer solche Angaben fest, weist er den Auftraggeber darauf hin.

3.4 Die verarbeiteten personenbezogenen Daten haben einen normalen Schutzbedarf; besondere Kategorien nach Art. 9 DSGVO, Finanz- oder Bonitätsdaten sind nicht Gegenstand der Verarbeitung. Die Parteien überprüfen diese Einschätzung, wenn sich Art oder Umfang der Verarbeitung wesentlich ändern.

4. Verantwortlichkeit und Verarbeitung auf dokumentierte Weisungen

4.1 Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung, verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO). Der Auftraggeber bestimmt die Zwecke und die wesentlichen Mittel der Verarbeitung. Dem Auftragnehmer verbleibt im Rahmen der dokumentierten Weisungen ein Entscheidungsspielraum hinsichtlich nicht wesentlicher technischer und organisatorischer Mittel der Leistungserbringung.

4.2 Die Weisungen werden anfänglich durch den Hauptvertrag und den vorgesehenen Funktionsumfang der Plattform festgelegt. Die Nutzung der Plattform in diesem Funktionsumfang gilt als Weisung. Der Auftraggeber kann die Weisungen danach in Textform (z. B. per E-Mail) durch einzelne Weisungen ändern (Einzelweisung). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere auf die Möglichkeit der Leistungserbringung, Termine und Vergütung, ergeben.

4.3 Ist dem Auftragnehmer die Umsetzung einer Weisung nicht zumutbar, ist er berechtigt, die Verarbeitung zu beenden und den Hauptvertrag außerordentlich zu kündigen. Die Entgeltspflicht des Auftraggebers entfällt mit der Einstellung der Leistung. Eine Unzumutbarkeit liegt insbesondere vor, wenn die Plattform als von mehreren Auftraggebern gemeinsam genutzte Infrastruktur betrieben wird und eine Änderung der Verarbeitung für einen einzelnen Auftraggeber technisch nicht möglich oder nicht zumutbar ist.

4.4 Weisungsberechtigt auf Seiten des Auftraggebers sind dessen gesetzliche Vertreter sowie die Personen, die der Auftraggeber dem Auftragnehmer in Textform als weisungsberechtigt benennt. Zum Empfang von Weisungen berechtigt sind auf Seiten des Auftragnehmers die Gesellschafter, erreichbar unter info@gutachterbook.de. Änderungen bei den weisungsberechtigten Personen zeigt der Auftraggeber dem Auftragnehmer unverzüglich in Textform an. Weisungen, auch mündliche, sind von beiden Parteien zu dokumentieren und mindestens für die Dauer des Auftragsverhältnisses aufzubewahren.

4.5 Die vertraglich vereinbarte Datenverarbeitung findet ausschließlich in der Bundesrepublik Deutschland statt. Eine Verlagerung der Verarbeitung in einen Drittstaat oder an eine internationale Organisation bedarf der vorherigen Zustimmung des Auftraggebers in Textform und darf nur erfolgen, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

4.6 Auskünfte an Dritte oder an betroffene Personen erteilt der Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers in Textform, es sei denn, er ist nach dem Recht der Europäischen Union oder eines Mitgliedstaats zur Herausgabe verpflichtet. Kopien und Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt; hiervon ausgenommen sind Sicherungskopien nach Anhang 3.

5. Rechte des Auftraggebers, Pflichten des Auftragnehmers

5.1 Der Auftragnehmer darf Daten betroffener Personen nur aufgrund dokumentierter Weisungen des Auftraggebers verarbeiten. Keine Weisungsbindung liegt vor, wenn ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a DSGVO gegeben ist (Verpflichtung nach dem Recht der Europäischen Union oder eines Mitgliedstaats). Besteht eine Verarbeitungspflicht entgegen einer Weisung, informiert der Auftragnehmer den Auftraggeber vor der Verarbeitung über die entsprechende rechtliche Anforderung, es sei denn, das betreffende Recht verbietet eine solche Information wegen eines wichtigen öffentlichen Interesses. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Datenschutzvorschriften verstößt. Er darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

5.2 Der Auftragnehmer gewährleistet, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Personen die Daten nur auf Weisung verarbeiten und sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Mit der Verarbeitung befasst sind derzeit

ausschließlich die Gesellschafter des Auftragnehmers. Künftige Beschäftigte werden vor Aufnahme ihrer Tätigkeit auf die Vertraulichkeit sowie die Weisungs- und Zweckbindung verpflichtet und über die maßgeblichen Datenschutzvorschriften unterrichtet. Die Vertraulichkeitspflicht besteht auch nach Beendigung der Tätigkeit und des Auftrags fort. Der Auftragnehmer weist die Verpflichtung dem Auftraggeber auf Wunsch nach.

5.3 Eine Verarbeitung der Daten zu eigenen Zwecken des Auftragnehmers findet nicht statt. Der Auftraggeber weist den Auftragnehmer an, aus den Daten anonyme, nicht auf Personen rückführbare Statistiken zur Verbesserung der Plattform zu erstellen; die dafür erforderliche Anonymisierung erfolgt im Auftrag des Auftraggebers und unterliegt dieser Vereinbarung. Nur die anonymisierten Ergebnisse, die keinen Personenbezug mehr aufweisen, nutzt der Auftragnehmer zu eigenen Zwecken.

5.4 Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Ansprüche betroffener Personen nach Kapitel III der DSGVO. Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragung nimmt der Auftraggeber im Regelfall selbst über die dafür vorgesehenen Funktionen der Plattform vor. Die nach Art. 28 Abs. 3 lit. e DSGVO geschuldete Unterstützung ist mit der vereinbarten Vergütung für die Plattform abgegolten, soweit sie mit den vorgesehenen Funktionen der Plattform oder mit üblichem Verwaltungsaufwand erbracht werden kann. Für darüber hinausgehende, vom Auftraggeber veranlasste Unterstützungsleistungen, die einen außergewöhnlichen zusätzlichen Aufwand verursachen, kann der Auftragnehmer eine angemessene, dem tatsächlichen Aufwand entsprechende Vergütung verlangen, sofern der zusätzliche Aufwand nicht auf einem Gesetzes- oder Vertragsverstoß des Auftragnehmers beruht. Der Auftragnehmer informiert den Auftraggeber vor Entstehung vergütungspflichtigen Aufwands über die voraussichtlichen Kosten.

5.5 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, insbesondere bei der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Datenschutz-Folgenabschätzung und der vorherigen Konsultation der Aufsichtsbehörde. Die Unterstützung nach dieser Ziffer ist mit der vereinbarten Vergütung für die Plattform abgegolten, soweit sie mit üblichem Verwaltungsaufwand erbracht werden kann. Für darüber hinausgehenden, vom Auftraggeber veranlassten außergewöhnlichen Zusatzaufwand gilt Ziffer 5.4 entsprechend.

5.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten des Auftraggebers mit den zu diesem Zeitpunkt verfügbaren Angaben, spätestens jedoch innerhalb von 48 Stunden. Die Frist begrenzt die Erstmeldung nach oben; sie rechtfertigt kein Zuwarten. Die Meldung erfolgt in Textform an die vom Auftraggeber in seinem Nutzerkonto hinterlegte E-Mail-Adresse und enthält, soweit bekannt, eine Beschreibung der Art der Verletzung mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen oder vorgeschlagenen Maßnahmen sowie eine Ansprechperson. Sind noch nicht alle Angaben verfügbar, meldet der Auftragnehmer zunächst den bekannten Sachverhalt und reicht die übrigen Angaben unverzüglich nach. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und dokumentiert die Verletzung. Meldungen an die Aufsichtsbehörde (Art. 33 DSGVO) und Benachrichtigungen betroffener Personen (Art. 34 DSGVO) obliegen dem Auftraggeber; der Auftragnehmer nimmt sie für den Auftraggeber nur nach dessen Weisung vor.

5.7 Der Auftragnehmer hat keinen Datenschutzbeauftragten benannt, da die Voraussetzungen des Art. 37 DSGVO und des § 38 BDSG nicht vorliegen. Ansprechpersonen für den Datenschutz sind die Gesellschafter, erreichbar unter info@gutachterbook.de. Die Benennung eines Datenschutzbeauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

5.8 Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde sowie über Anfragen, Ermittlungen oder sonstige Erkundigungen einer Aufsichtsbehörde, soweit sie die Verarbeitung für den Auftraggeber betreffen.

5.9 Der Auftragnehmer führt ein Verzeichnis aller Kategorien von im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dem Auftraggeber auf dessen Wunsch die Informationen zur Verfügung, die dieser für sein Verzeichnis nach Art. 30 Abs. 1 DSGVO benötigt. Die Parteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO).

5.10 Machen betroffene Personen Schadensersatzansprüche nach Art. 82 DSGVO geltend, unterstützen sich die Parteien gegenseitig im erforderlichen Umfang bei der Aufklärung des Sachverhalts und der Bearbeitung der Ansprüche.

6. Pflichten des Auftraggebers

6.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Durchführung des Auftrags Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

6.2 Der Auftraggeber ist für das Vorliegen einer Rechtsgrundlage für die Verarbeitung sowie für die Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO gegenüber seinen Kunden und den weiteren betroffenen Personen verantwortlich.

6.3 Der Auftraggeber stellt sicher, dass die Zugangsdaten seiner Nutzerkonten vertraulich behandelt werden, dass die Berechtigungen seiner Beschäftigten dem tatsächlichen Bedarf entsprechen und dass er dem Auftragnehmer unverzüglich mitteilt, wenn das Konto eines ausgeschiedenen Beschäftigten zu deaktivieren ist; der Auftragnehmer deaktiviert das Konto unverzüglich nach Zugang der Mitteilung.

6.4 Auf Anforderung des Auftragnehmers benennt der Auftraggeber eine Ansprechperson in Datenschutzangelegenheiten. Verfügt der Auftraggeber über einen Datenschutzbeauftragten, teilt er dessen Kontaktdaten mit.

6.5 Der Auftraggeber führt das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO für die von ihm verantworteten Verarbeitungen.

6.6 Der Auftraggeber trägt dafür Sorge, dass er die Daten, für die ihn eigene gesetzliche Aufbewahrungspflichten treffen – insbesondere erstellte Gutachten –, innerhalb der Exportfrist nach Ziffer 11.3 aus der Plattform exportiert. Der Auftraggeber kann Daten, die er in der Plattform gespeichert hat, bereits vor Vertragsbeendigung selbst löschen.

7. Anfragen betroffener Personen

7.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jeden Antrag, den er von einer betroffenen Person erhalten hat, und leitet ihn an den Auftraggeber weiter. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Auftraggeber dazu ermächtigt.

7.2 Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten, und befolgt dabei die Weisungen des Auftraggebers. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8. Maßnahmen zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO

8.1 Der Auftragnehmer ergreift in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und der Schutz der Rechte und Freiheiten der betroffenen Personen gewährleistet ist. Der Auftraggeber ergreift in seinem Verantwortungsbereich gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, insbesondere für die von ihm genutzten Endgeräte, Netzzugänge und Zugangsdaten.

8.2 Die technischen und organisatorischen Maßnahmen des Auftragnehmers sind in Anhang 3 beschrieben. Anhang 3 ist Bestandteil dieser Vereinbarung. Maßnahmen, die in Anhang 3 als „geplant“ bezeichnet sind, sind zum Stand dieser Vereinbarung nicht umgesetzt; der Auftragnehmer informiert den Auftraggeber über ihre Umsetzung nach Ziffer 8.4.

8.3 Der Auftragnehmer betreibt ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 lit. d DSGVO. Anhang 3 wird mindestens jährlich sowie bei wesentlichen Änderungen der Plattform überprüft und fortgeschrieben.

8.4 Der Auftragnehmer passt die getroffenen Maßnahmen im Laufe der Zeit an die Entwicklung des Stands der Technik und die Risikolage an. Eine Änderung der Maßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das Schutzniveau nach Art. 32 DSGVO nicht unterschritten wird. Wesentliche Änderungen dokumentiert

der Auftragnehmer und teilt sie dem Auftraggeber in Textform mit; die jeweils aktuelle Fassung des Anhangs 3 wird unter der in Ziffer 13.8 genannten Adresse bereitgestellt.

8.5 Der Auftragnehmer unterhält keine Betriebsräume, in denen personenbezogene Daten des Auftraggebers verarbeitet werden. Die Plattform wird im Rechenzentrum des in Anhang 2 genannten Subunternehmers betrieben. Administrative Tätigkeiten führen die Gesellschafter des Auftragnehmers im Wege mobiler Arbeit von persönlichen Endgeräten aus, die den in Anhang 3 Nr. 8 beschriebenen Maßnahmen unterliegen. Der Auftraggeber stimmt dieser Verarbeitungssituation mit Abschluss dieser Vereinbarung zu.

9. Nachweis und Überprüfung

9.1 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht im Einzelfall Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem von diesem beauftragten Prüfer durchgeführt werden. Der Auftragnehmer ist berechtigt, eine Verschwiegenheitserklärung vom Auftraggeber und von dessen beauftragtem Prüfer zu verlangen, die den Auftraggeber jedoch nicht daran hindert, selbst Nachweise gegenüber der für ihn zuständigen Aufsichtsbehörde zu erbringen. Unmittelbare Wettbewerber des Auftragnehmers oder Personen, die für unmittelbare Wettbewerber tätig sind, kann der Auftragnehmer als Prüfer ablehnen.

9.2 Als Nachweis dienen vorrangig Auskünfte des Auftragnehmers in Textform, die Beschreibung der Maßnahmen nach Anhang 3 sowie die Nachweise und Zertifizierungen des in Anhang 2 genannten Rechenzentrumsbetreibers, insbesondere dessen Zertifizierung nach ISO 27001. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über den Widerruf oder die wesentliche Änderung solcher Nachweise.

9.3 Da der Auftragnehmer keine Betriebsräume mit Daten des Auftraggebers unterhält (Ziffer 8.5), erfolgen Überprüfungen vorrangig durch Auskunft in Textform sowie, soweit erforderlich, durch Vorführung der Systeme per Fernzugriff zu einem vereinbarten Termin. Eine Inspektion beim Rechenzentrumsbetreiber richtet sich nach dessen Bedingungen; der Auftragnehmer unterstützt den Auftraggeber dabei im zumutbaren Umfang. Überprüfungen sind mit angemessener Frist von mindestens zwei Wochen anzukündigen und zu den üblichen Geschäftszeiten ohne übermäßige Störung des Betriebsablaufs durchzuführen, sofern nicht eine Kontrolle ohne Ankündigung erforderlich erscheint, weil andernfalls der Kontrollzweck gefährdet wäre. Der Auftragnehmer wirkt aktiv an der Durchführung der Kontrolle mit.

9.4 Für Informationen und Unterstützungshandlungen im Rahmen von Überprüfungen ohne konkreten Anlass, deren Aufwand einen Arbeitstag übersteigt, kann der Auftragnehmer eine angemessene Vergütung verlangen, soweit die Kontrolle nicht wegen eines Gesetzes- oder Vertragsverstoßes des Auftragnehmers erforderlich wurde. Der Auftragnehmer lässt dem Auftraggeber vorab eine Kosteninformation zukommen. Die Ausübung der gesetzlichen Kontroll- und Nachweisrechte des Auftraggebers darf durch eine Vergütungspflicht weder verhindert noch unangemessen erschwert werden.

9.5 Einem Datenschutzbeauftragten des Auftraggebers stehen zur Erfüllung seiner gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag die Rechte nach den Ziffern 9.1 bis 9.3 in gleicher Weise zu.

10. Subunternehmer (weitere Auftragsverarbeiter)

10.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 Abs. 2 DSGVO (Subunternehmer) zur Vertragserfüllung einzusetzen.

10.2 Die aktuell eingesetzten Subunternehmer sind in Anhang 2 aufgeführt. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.

10.3 Der Auftragnehmer informiert den Auftraggeber mindestens vier Wochen im Voraus in Textform, wenn er eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern beabsichtigt, und stellt ihm die Informationen zur Verfügung, die er zur Ausübung seines Einspruchsrechts benötigt.

10.4 Der Auftraggeber kann gegen die beabsichtigte Änderung innerhalb von zwei Wochen nach Zugang der Information aus einem wichtigen, datenschutzrechtlichen Grund in Textform Einspruch erheben. Erfolgt kein Einspruch, gilt die Änderung als genehmigt. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die

Änderung für ihn nicht zumutbar ist – die von der Änderung betroffene Leistung innerhalb einer angemessenen Frist von mindestens vier Wochen nach Zugang des Einspruchs einstellen und den Hauptvertrag außerordentlich kündigen. Mit dem Zeitpunkt der Leistungseinstellung entfällt die Entgeltspflicht des Auftraggebers. Das Recht des Auftraggebers, den Hauptvertrag im Fall des Einspruchs seinerseits außerordentlich zu kündigen, bleibt unberührt.

10.5 Erteilt der Auftragnehmer Aufträge an Subunternehmer, obliegt es ihm, seine datenschutzrechtlichen Pflichten aus dieser Vereinbarung durch einen Vertrag nach Art. 28 Abs. 4 DSGVO auf den Subunternehmer zu übertragen. Eine Weitergabe von Daten an einen Subunternehmer erfolgt erst nach Abschluss dieses Vertrags. Der Auftragnehmer stellt insbesondere durch regelmäßige Überprüfungen sicher, dass die Subunternehmer die technischen und organisatorischen Maßnahmen einhalten. Kommt ein Subunternehmer seinen Pflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Subunternehmers. Der Auftraggeber kann in Textform Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers verlangen.

10.6 Nicht als Subunternehmerleistungen im Sinne dieser Regelung gelten Nebenleistungen, die der Auftragnehmer zur Ausübung seiner Tätigkeit in Anspruch nimmt und bei denen der Dritte keinen Zugriff auf personenbezogene Daten des Auftraggebers hat, wie Telekommunikations- und Postdienstleistungen, Wartung ohne Datenzugriff sowie die Entsorgung von Datenträgern. Erhält ein Dritter im Rahmen einer solchen Leistung Zugriff auf personenbezogene Daten des Auftraggebers, gilt er als Subunternehmer nach den Ziffern 10.1 bis 10.5. Der Auftragnehmer ist auch insoweit verpflichtet, angemessene Vereinbarungen und Kontrollmaßnahmen zum Schutz der Daten zu treffen.

11. Löschung und Rückgabe von Daten

11.1 Die Hoheit über die im Auftrag verarbeiteten Daten liegt ausschließlich beim Auftraggeber als Verantwortlichem.

11.2 Während der Laufzeit löscht der Auftraggeber Daten über die dafür vorgesehene Löschfunktion der Plattform. Darüber hinausgehende Löschungen führt der Auftragnehmer auf Weisung des Auftraggebers durch.

11.3 Nach Beendigung des Hauptvertrags löscht der Auftragnehmer nach Wahl des Auftraggebers sämtliche im Auftrag verarbeiteten personenbezogenen Daten oder gibt sie zurück, sofern nicht nach dem Recht der Europäischen Union oder eines Mitgliedstaats eine Verpflichtung zur Speicherung besteht (Ziffer 11.6). Zur Ausübung dieses Wahlrechts stellt der Auftragnehmer dem Auftraggeber dessen Daten für die Dauer von 30 Tagen nach Vertragsende zum Export bereit (Rückgabe): Der Auftraggeber kann Kunden-, Leistungs- und Gutachtendaten über die Plattform als CSV-Datei exportieren sowie Gutachten und Schadensfotos einzeln herunterladen; auf Anforderung in Textform stellt der Auftragnehmer innerhalb der Exportfrist zusätzlich ein Gesamtarchiv aller Gutachten und Schadensfotos des Auftraggebers bereit. Verlangt der Auftraggeber innerhalb dieser Frist in Textform die Löschung, löscht der Auftragnehmer die Daten unverzüglich.

11.4 Macht der Auftraggeber innerhalb der Exportfrist von seinem Wahlrecht keinen Gebrauch, gilt die Löschung als gewählt. Der Auftragnehmer löscht in diesem Fall nach Ablauf der Frist sämtliche Daten des Auftraggebers im Produktivsystem. Die Löschung wird dem Auftraggeber auf Anforderung in Textform bestätigt (Löschprotokoll).

11.5 Sicherungskopien werden rollierend erstellt und im regulären Sicherungszyklus nach Anhang 3 überschrieben. Gelöschte Daten sind dadurch spätestens zehn Tage nach ihrer Löschung im Produktivsystem auch in allen Sicherungskopien nicht mehr vorhanden. Eine gezielte Löschung einzelner Datensätze aus bestehenden Sicherungskopien erfolgt nicht. Eine Wiederherstellung aus Sicherungskopien findet nur zur Wiederherstellung des Gesamtsystems statt; bereits gelöschte Daten werden in diesem Fall unverzüglich erneut gelöscht.

11.6 Von der Löschung ausgenommen sind ausschließlich Daten, die der Auftragnehmer zur Abrechnung des Hauptvertrags aufgrund gesetzlicher Aufbewahrungspflichten (insbesondere § 147 AO, § 257 HGB) aufbewahren muss, sowie Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung dienen (insbesondere Weisungen, Vorfalldokumentation, Löschprotokolle). Diese Ausnahme betrifft keine Daten der Kunden des Auftraggebers oder anderer betroffener Personen nach Ziffer 3.2. Nach Ablauf der jeweiligen Aufbewahrungsfrist gilt Ziffer 11.4.

12. Haftung und Schadensersatz

12.1 Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Fall der Geltendmachung eines Schadensersatzanspruchs durch eine betroffene Person nach Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrunde liegenden Sachverhalts beizutragen.

12.2 Die im Hauptvertrag vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter nach Art. 82 DSGVO, soweit nicht ausdrücklich etwas anderes vereinbart ist.

12.3 Der Auftragnehmer haftet gegenüber dem Auftraggeber nicht für Schäden, die darauf beruhen, dass der Auftraggeber seinen Pflichten nach Ziffer 6 nicht nachgekommen ist, insbesondere wenn eine Verarbeitung ohne ausreichende Rechtsgrundlage erfolgt oder die Informationspflichten gegenüber den betroffenen Personen nicht erfüllt wurden.

13. Vertragslaufzeit, Änderungen, Sonstiges

13.1 Diese Vereinbarung kommt mit der Annahme der Nutzungsbedingungen der Plattform durch den Auftraggeber oder, sofern die Parteien dies wünschen, mit beidseitiger Unterzeichnung nach Anhang 4 zustande. Sie endet mit dem Ende des Hauptvertrags; Ziffer 1.4 Satz 2 bleibt unberührt.

13.2 Der Auftragnehmer ist berechtigt, diese Vereinbarung mit angemessener Ankündigungsfrist zu ändern, soweit die Änderung aufgrund einer Änderung der Rechtslage, einer verbindlichen behördlichen oder gerichtlichen Vorgabe, einer Änderung der Verarbeitungstätigkeiten oder der technischen bzw. organisatorischen Ausgestaltung der Plattform erforderlich ist und das vertragliche Gleichgewicht sowie das Schutzniveau der betroffenen Personen hierdurch nicht zum Nachteil des Auftraggebers beeinträchtigt werden. Der Auftragnehmer weist den Auftraggeber in der Änderungsankündigung gesondert auf die Bedeutung der Änderung hin und räumt ihm eine Frist von mindestens sechs Wochen zur Erklärung eines Widerspruchs in Textform ein. Er weist darauf hin, dass die Änderung wirksam wird, wenn der Auftraggeber nicht binnen der gesetzten Frist widerspricht. Im Fall eines Widerspruchs steht beiden Parteien ein außerordentliches Kündigungsrecht zu. Änderungen, die das Schutzniveau für die betroffenen Personen absenken, sind auf diesem Weg ausgeschlossen.

13.3 Diese Vereinbarung ist Bestandteil des Hauptvertrags. Bei etwaigen Widersprüchen gehen die Regelungen dieser Vereinbarung den Regelungen des Hauptvertrags vor, soweit sie die Verarbeitung personenbezogener Daten betreffen. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

13.4 Der Auftraggeber stimmt bereits jetzt zu, dass diese Vereinbarung im Fall einer Umwandlung des Auftragnehmers oder der Einbringung seines Geschäftsbetriebs in eine andere Gesellschaft auf den Rechtsnachfolger übergeht, sofern dieser in sämtliche Rechte und Pflichten aus dieser Vereinbarung und dem Hauptvertrag eintritt. Der Auftragnehmer informiert den Auftraggeber über einen solchen Übergang in Textform.

13.5 Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist der Sitz des Auftragnehmers, sofern der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist. Ein etwaiger ausschließlicher gesetzlicher Gerichtsstand bleibt vorbehalten.

13.6 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, informiert der Auftragnehmer den Auftraggeber unverzüglich. Der Auftragnehmer weist alle in diesem Zusammenhang Verantwortlichen unverzüglich darauf hin, dass die Hoheit an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegt.

13.7 Diese Vereinbarung kann gemäß Art. 28 Abs. 9 DSGVO in elektronischem Format abgeschlossen werden. Wünscht der Auftraggeber eine unterzeichnete Fassung, genügt der Austausch der nach Anhang 4 unterzeichneten Exemplare als PDF-Datei per E-Mail.

13.8 Die jeweils aktuelle Fassung dieser Vereinbarung einschließlich ihrer Anhänge ist online unter folgender Adresse abrufbar: <https://gutachterbook.de/avv>

Anhang 1 – Leistungsbeschreibung, Datenkategorien und betroffene Personen

zur Vereinbarung zur Auftragsverarbeitung der GutachterBook – Faik-Salih Cansu & Sebastian Fröhlich GbR ·
Version 1.0 · Stand 09/2026

1. Leistungen des Auftragnehmers im Auftrag des Auftraggebers

Nr.	Leistung	Beschreibung
1	Online-Terminvergabe	Endkunden buchen über die Plattform Termine bei dem Auftraggeber; der Auftraggeber verwaltet Terminanfragen, Bestätigungen und Absagen. Terminbestätigungen und Erinnerungen werden per E-Mail an die betroffene Person versandt.
2	Kunden- und Fahrzeugverwaltung	Erfassung, Speicherung und Pflege der Stammdaten der Kunden des Auftraggebers sowie der zugehörigen Fahrzeugdaten.
3	Schadensdokumentation	Erfassung von Schadensbeschreibungen und Ablage von Schadensfotos zu einem Vorgang.
4	Gutachtenverwaltung	Erstellung, Ablage und Übermittlung von Gutachten als PDF-Datei; Zuordnung zu Kunde, Fahrzeug und Vorgang.
5	Nutzerkonten des Auftraggebers	Bereitstellung von Nutzerkonten für Beschäftigte des Auftraggebers; alle Konten eines Büros haben dieselben Berechtigungen. Anlage und Deaktivierung der Konten nimmt der Auftragnehmer auf Anforderung des Auftraggebers vor.
6	Datenexport und Löschung	Export der Kunden-, Leistungs- und Gutachtendaten als CSV-Datei, Einzeldownload von Gutachten und Schadensfotos, Gesamtarchiv auf Anforderung (Ziffer 11.3) sowie Löschfunktion für einzelne Personen und Vorgänge (Ziffer 11.2).

2. Kategorien personenbezogener Daten

Nr.	Datenkategorie	Einzelangaben
1	Stammdaten	Vor- und Nachname, Anschrift, E-Mail-Adresse, Telefonnummer
2	Fahrzeugdaten	Marke, Modell, amtliches Kennzeichen sowie weitere Fahrzeugmerkmale, soweit vom Auftraggeber erfasst
3	Schadensdaten	Schadensbeschreibung, Schadensschwere, Fotos des Fahrzeugs
4	Vorgangsdaten	Termine, Buchungsstatus, erstellte Gutachten (PDF-Dateien)
5	Notizen	Interne Notizen des Auftraggebers als Freitext
6	Zugangsdaten	E-Mail-Adresse und Passwort (ausschließlich als kryptografischer Hashwert) der Nutzerkonten des Auftraggebers
7	Nutzungs- und Verbindungsdaten	IP-Adresse, Zeitstempel, Browserkennung, die beim technischen Betrieb anfallen

3. Kategorien betroffener Personen

Nr.	Personengruppe	Erläuterung
1	Kunden des Auftraggebers	Fahrzeughalter und Auftraggeber von Gutachten
2	Interessenten	Personen, die über die Plattform einen Termin bei dem Auftraggeber buchen
3	Beschäftigte des Auftraggebers	Nutzer der Plattform mit eigenem Nutzerkonto
4	Weitere Personen eines Schadensvorgangs	Personen, deren Daten der Auftraggeber im Rahmen eines Schadensvorgangs erfasst, z. B. weitere Unfallbeteiligte, Fahrzeughalter, Versicherungsnehmer

Anhang 2 – Subunternehmer (weitere Auftragsverarbeiter)

zur Vereinbarung zur Auftragsverarbeitung der GutachterBook – Faik-Salih Cansu & Sebastian Fröhlich GbR ·
Version 1.0 · Stand 09/2026

Nach Ziffer 10.2 der Vereinbarung sind die zur Erfüllung des Hauptvertrags bereits hinzugezogenen Subunternehmer zu bezeichnen. Der Auftraggeber erklärt sich mit deren Beauftragung einverstanden. Änderungen richten sich nach den Ziffern 10.3 und 10.4.

Nr.	Subunternehmer (Name, Anschrift)	Datum des Abschlusses der Vereinbarung zur Auftragsverarbeitung	(Teil-)Leistungsgegenstand im Rahmen der Auftragsverarbeitung	Ort der Verarbeitung
1	IONOS SE Elgendorfer Straße 57 56410 Montabaur	23.09.2026 (Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO, Bestandteil der Allgemeinen Geschäftsbedingungen der IONOS SE)	Betrieb des Servers, auf dem Anwendung, Datenbank, Dateiablage und Sicherungskopien der Plattform gespeichert werden (Hosting); Versand von E-Mails an Kunden und Beschäftigte des Auftraggebers (Terminbestätigungen, Erinnerungen, Kontoverwaltung)	Deutschland

Weitere Subunternehmer werden nicht eingesetzt. Insbesondere erfolgen keine Zahlungsabwicklung über Dritte, keine externe Fehler- oder Verfügbarkeitsüberwachung und keine Auswertung durch Analysedienste. Eine Übermittlung personenbezogener Daten in Drittstaaten findet nicht statt.

Nachweise des Subunternehmers: Die IONOS SE weist die Sicherheit ihrer Rechenzentren durch eine Zertifizierung nach ISO 27001 nach. Das jeweils aktuelle Zertifikat stellt die IONOS SE auf ihrer Website bereit; der Auftragnehmer legt es dem Auftraggeber auf Anforderung vor (Ziffer 9.2).

Anhang 3 – Technische und organisatorische Maßnahmen (TOM)

zur Vereinbarung zur Auftragsverarbeitung der GutachterBook – Faik-Salih Cansu & Sebastian Fröhlich GbR ·
Version 1.0 · Stand 09/2026

Ziffer 8 der Vereinbarung verweist zur Konkretisierung der technischen und organisatorischen Maßnahmen auf diesen Anhang. Der Auftragnehmer betreibt die Plattform auf einem Server im Rechenzentrum des in Anhang 2 genannten Subunternehmers; er unterhält keine eigenen Betriebsräume, in denen personenbezogene Daten des Auftraggebers verarbeitet werden. Die nachfolgende Übersicht folgt der Gliederung des Anhangs II der Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/915). Maßnahmen, die als *geplant* gekennzeichnet sind, sind zum Stand dieses Anhangs nicht umgesetzt.

Nr.	Maßnahme	Umsetzung bei GutachterBook
1	Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten	Transportverschlüsselung: Zugriff auf die Plattform ausschließlich über HTTPS (TLS). Passwörter werden ausschließlich als bcrypt-Hashwert gespeichert, nie im Klartext. Verschlüsselung der Datenbankinhalte und Sicherungskopien im Ruhezustand: <i>geplant</i> ; bis zur Umsetzung ergibt sich der Schutz aus der Zugangsbeschränkung nach Nr. 5 und 7. Eine weitergehende Pseudonymisierung ist wegen des Zwecks der Verarbeitung (namentliche Kundenverwaltung) nicht vorgesehen.
2	Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste	Mandantentrennung auf Datenebene: Jeder Datensatz ist einem Sachverständigenbüro zugeordnet; jede Abfrage prüft diese Zuordnung; Datensätze anderer Büros werden als nicht vorhanden behandelt. Rollenmodell mit getrennten Rollen für Endkunden, Beschäftigte des Auftraggebers und Plattform-Administration. Jede ändernde Aktion ist gegen untergeschobene Anfragen fremder Webseiten (CSRF) abgesichert. Hochgeladene Dateien werden auf Bildformat und tatsächlichen Dateinhalt geprüft, auf 8 MB begrenzt und unter einem neu vergebenen Namen gespeichert. Verfügbarkeit der Infrastruktur (Stromversorgung, Klimatisierung, Netzanbindung, Redundanz) nach dem Betriebskonzept des Rechenzentrumsbetreibers.
3	Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	Automatische Sicherung der Datenbank sowie der abgelegten Gutachten und Schadensfotos einmal täglich um 03:00 Uhr. Es werden höchstens zehn Sicherungsgenerationen rollierend vorgehalten; jede neue Sicherung ersetzt die jeweils älteste, eine zusätzliche Größenbegrenzung kann ältere Sicherungen früher entfernen. Die Sicherungen liegen in einem von der Anwendung getrennten Speicherbereich (eigenes Volume) auf demselben Server und überdauern einen Neuaufbau der Anwendung. Zusätzliche Kopie der Sicherungen auf einem getrennten System: <i>geplant</i> . Sicherungsdateien können weder über die Anwendung heruntergeladen noch über sie gelöscht werden; der Zugriff setzt administrativen Serverzugang voraus. Eine dokumentierte Wiederherstellungsanleitung liegt vor; die Wiederherstellung aus einer Sicherung wird mindestens einmal jährlich auf dem Testsystem erprobt.
4	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen	Dieser Anhang wird mindestens jährlich sowie bei wesentlichen Änderungen der Plattform überprüft und fortgeschrieben. Änderungen an der Plattform werden vor der Auslieferung mit einer automatisierten Testsuite (rund 3.400 Testfälle) geprüft, die ausdrücklich Testfälle zur Mandantentrennung und zum Schutz vor eingeschleustem Fremdcode (Injection) enthält. Sicherheitsvorfälle werden eingegrenzt, dokumentiert, ausgewertet und nach Ziffer 5.6 gemeldet.

5	Maßnahmen zur Identifizierung und Autorisierung der Nutzer	Zugang zur Plattform nur mit persönlichem Nutzerkonto und Passwort; eine Mindestlänge von acht Zeichen und Regeln zur Zeichenzusammensetzung werden erzwungen. Berechtigungen nach Rollenmodell (Nr. 2); Beschäftigte des Auftraggebers sehen ausschließlich Daten ihres Büros. Administrativer Zugriff auf Server und Datenbank ausschließlich für die Gesellschafter über persönliche SSH-Schlüssel; kein Zugang Dritter. Zwei-Faktor-Authentisierung für Nutzerkonten: <i>geplant</i> .
6	Maßnahmen zum Schutz der Daten während der Übermittlung	Ausschließlich HTTPS zwischen Endgerät und Plattform. E-Mails an betroffene Personen werden über den Subunternehmer nach Anhang 2 transportverschlüsselt versandt. Eine Weitergabe auf physischen Datenträgern findet nicht statt. Schadensfotos werden nur nach Anmeldung und Prüfung von Rolle und Büro-Zugehörigkeit ausgeliefert.
7	Maßnahmen zum Schutz der Daten während der Speicherung	Die Datenbank ist nur aus dem internen Netz der Anwendung erreichbar und hat keinen von außen erreichbaren Port. Auf dem Produktivsystem ist keine Datenbank-Weboberfläche installiert. Schadensfotos und Gutachten liegen außerhalb des öffentlich ausgelieferten Verzeichnisses. Verschlüsselung im Ruhezustand: siehe Nr. 1 (<i>geplant</i>).
8	Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden	Die Server befinden sich im Rechenzentrum des Subunternehmers nach Anhang 2; Zutrittsregelung, Überwachung und Brandschutz erfolgen nach dessen Sicherheitskonzept (Zertifizierung nach ISO 27001). Der Auftragnehmer unterhält keine eigenen Betriebsräume mit Daten des Auftraggebers. Administrative Tätigkeiten erfolgen von persönlichen Endgeräten der Gesellschafter mit Festplattenverschlüsselung, Bildschirm Sperre und aktuellem Betriebssystem; auf den Endgeräten werden keine Kopien der Daten des Auftraggebers abgelegt.
9	Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen	Der aktuelle Status einer Terminbuchung wird zusammen mit dem Zeitpunkt ihrer Anlage und einer etwaigen Verschiebung gespeichert; eine vollständige Änderungshistorie je Buchung: <i>geplant</i> . Der Webserver protokolliert Zugriffe auf die Plattform (IP-Adresse, Zeitstempel, aufgerufene Adresse); die Protokolle werden täglich rotiert und spätestens nach 15 Tagen automatisch gelöscht. Revisionssichere Protokollierung, welcher Nutzer welchen Datensatz gelesen hat: <i>geplant</i> .
10	Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration	Entwicklung und Test finden auf einem getrennten System mit eigenen Testdaten statt. Auf dem Produktivsystem sind nur die für den Betrieb erforderlichen Dienste installiert und nur die erforderlichen Netzwerkports erreichbar. Sicherheitsaktualisierungen des Betriebssystems werden regelmäßig eingespielt.
11	Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit	Beide Gesellschafter sind gemeinsam für Datenschutz und IT-Sicherheit zuständig und über info@gutachterbook.de erreichbar. Ein Datenschutzbeauftragter ist nicht benannt (§ 38 BDSG). Der Auftragnehmer führt ein Verzeichnis nach Art. 30 Abs. 2 DSGVO. Weisungen des Auftraggebers werden dokumentiert. Subunternehmer werden nur nach Abschluss eines Vertrags nach Art. 28 Abs. 4 DSGVO eingesetzt.
12	Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten	Der Auftragnehmer verfügt über keine eigene Zertifizierung. Die Sicherheit der Infrastruktur ist durch die Zertifizierung des Rechenzentrumsbetreibers nach ISO 27001 nachgewiesen. Die Qualität der Plattform wird durch die automatisierte Testsuite nach Nr. 4 gesichert, die vor jeder Auslieferung ausgeführt wird.

13	Maßnahmen zur Gewährleistung der Datenminimierung	Die Plattform erhebt nur die für den jeweiligen Vorgang erforderlichen Angaben. Für besondere Kategorien personenbezogener Daten sind keine Felder vorgesehen. Es werden keine Analyse- oder Tracking-Dienste eingesetzt.
14	Maßnahmen zur Gewährleistung der Datenqualität	Eingaben werden bei der Erfassung auf Vollständigkeit der Pflichtfelder und auf Format geprüft (z. B. E-Mail-Adresse). Der Auftraggeber kann sämtliche Daten seiner Kunden jederzeit über die Oberfläche berichtigen.
15	Maßnahmen zur Gewährleistung einer begrenzten Speicherdauer	Der Auftraggeber löscht Personen und Vorgänge über die Löschfunktion der Plattform. Nach Vertragsende werden die Daten nach Ablauf der Exportfrist von 30 Tagen gelöscht (Ziffer 11). Sicherungskopien werden spätestens nach zehn Tagen überschrieben. Technische Protokolle werden spätestens nach 15 Tagen automatisch gelöscht.
16	Maßnahmen zur Gewährleistung der Rechenschaftspflicht	Dokumentation der Maßnahmen in diesem Anhang; Verzeichnis nach Art. 30 Abs. 2 DSGVO; Dokumentation von Weisungen, Sicherheitsvorfällen und Löschungen; Nachweise nach Ziffer 9.
17	Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung	Export der Kunden-, Leistungs- und Gutachtendaten als CSV-Datei über die Plattform; Einzeldownload von Gutachten und Schadensfotos; Gesamtarchiv auf Anforderung (Ziffer 11.3). Für die Löschung einer Person steht ein gesonderter Löschweg zur Verfügung, der zunächst alle zu dieser Person gespeicherten Datenbestände anzeigt und die Löschung erst nach ausdrücklicher Bestätigung ausführt. Löschung in Sicherungskopien nach Ziffer 11.5.
18	Maßnahmen zur Unterstützung des Verantwortlichen	Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragung) kann der Auftraggeber über die Funktionen der Plattform selbst erfüllen. Ansprechpersonen für den Datenschutz sind über info@gutachterbook.de erreichbar. Meldung von Verletzungen des Schutzes personenbezogener Daten nach Ziffer 5.6 innerhalb von 48 Stunden. Unterstützung bei Datenschutz-Folgenabschätzung und Anfragen der Aufsichtsbehörde nach Ziffer 5.5.

Anhang 4 – Annahme und Unterzeichnung

zur Vereinbarung zur Auftragsverarbeitung der GutachterBook – Faik-Salih Cansu & Sebastian Fröhlich GbR ·
Version 1.0 · Stand 09/2026

Diese Vereinbarung wird nach Ziffer 13.1 mit Annahme der Nutzungsbedingungen der Plattform Bestandteil des Hauptvertrags. Wünscht der Auftraggeber eine unterzeichnete Fassung, wird sie von beiden Parteien nachfolgend unterzeichnet. Der Austausch der unterzeichneten Exemplare als PDF-Datei per E-Mail genügt (Ziffer 13.7).

Auftraggeber (Verantwortlicher)

Firmierung / Name des
Sachverständigenbüros

Straße, Hausnummer

PLZ, Ort

Vertreten durch (Inhaber/in,
Geschäftsführung)

E-Mail für Weisungen und Meldungen

Ansprechperson Datenschutz (falls
abweichend)

Auftragnehmer (Auftragsverarbeiter)

Firmierung

GutachterBook – Faik-Salih Cansu & Sebastian Fröhlich GbR

Anschrift

Unter den Eichen 103, 40625 Düsseldorf

Vertreten durch

die Gesellschafter Faik-Salih Cansu und Sebastian Fröhlich,
gemeinschaftlich

E-Mail für Weisungen und Meldungen

info@gutachterbook.de

Datum, Ort

Datum, Ort

Unterschrift (Auftraggeber)

Unterschrift (Auftragnehmer) – Faik-Salih Cansu,
Gesellschafter

Name, Vorname, Funktion

Unterschrift (Auftragnehmer) – Sebastian Fröhlich,
Gesellschafter

Version 1.0

Stand: 09/2026

Dieses Dokument ist online unter folgender Adresse abrufbar:
<https://gutachterbook.de/avv>