Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

zwischen dem Verantwortlichen

– nachfolgend „Auftraggeber“ –

und dem Auftragsverarbeiter

Justin LegalTech GmbH, Columbiadamm 37, 10965 Berlin

– nachfolgend „Auftragnehmerin“ –

1. Allgemeine Bestimmungen und Vertragsgegenstand

1.1 Für diesen Auftragsverarbeitungsvertrag gelten die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO“), insbesondere des Art. 4 DSGVO.

1.2 Die Auftragnehmerin stellt dem Auftraggeber eine SaaS-Lösung zur Verfügung, in der neben den Daten des Auftraggebers auch Daten der Kunden des Auftraggebers verarbeitet werden können (insb. Daten von Mandanten von Rechtsanwaltskanzleien). Die Auftragnehmerin verarbeitet im Rahmen der Erbringung der vereinbarten Leistungen personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Auftrags.

1.3 Im Rahmen der Auftragsverarbeitung verarbeitet die Auftragnehmerin insbesondere folgende Datenkategorien:

- Stammdaten, Namen, Adressen, Kontaktdaten (E-Mail-Adresse, Telefonnummer etc.);
- personenbezogene Daten aus laufenden oder anstehenden Gerichts- oder Behördenverfahren;
- personenbezogene Daten zu Zivil-, Straf- oder Ordnungswidrigkeitenverfahren;
- personenbezogene Daten zu gerichtlichen oder außergerichtlichen Rechtsstreitigkeiten;
- personenbezogene Daten aus sich anbahnenden oder geschlossenen Verträgen;
- sonstige personenbezogenen Daten, die mit der Anbahnung von Mandatsbeziehungen zwischen Mandant und Rechtsanwalt verbunden sind.

1.4 Von der Auftragsverarbeitung sind insbesondere folgende Personenkategorien betroffen:

- Mandanten und potenzielle Mandanten des Auftraggebers
- Gegner des Mandanten / des potenziellen Mandanten (bei rechtlichen Streitigkeiten)
- Dritte, die in irgendeiner Weise am betreffenden rechtlichen Sachverhalt beteiligt sind und vom (potenziellen) Mandanten benannt werden.

1.5 Die Verarbeitung der Daten durch die Auftragnehmerin findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Vor Verlagerung der Verarbeitung in ein Drittland informiert die

Auftragnehmerin den Auftraggeber in Textform (bspw. per E-Mail). Der Auftraggeber kann der Änderung innerhalb von 3 Wochen ab Erhalt der Information durch die Auftragnehmerin in schriftlicher Form oder in Textform (bspw. per E-Mail) begründet widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Die Verlagerung der Verarbeitung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

2. Laufzeit und Kündigung

Die Laufzeit der Auftragsverarbeitung richtet sich nach der Laufzeit des Hauptvertrags. Soweit und solange nach Beendigung des Hauptvertrags personenbezogene Daten des Auftraggebers im Auftrag weiterverarbeitet werden, gilt diese Vereinbarung bis zu dem Zeitpunkt, zu dem die Verarbeitung dieser Daten durch die Auftragnehmerin endet. Das Recht auf außerordentliche fristlose Kündigung aus wichtigem Grund bleibt hiervon unberührt.

3. Rechte und Pflichten des Auftraggebers

3.1 Die Verarbeitung der vertragsgegenständlichen Daten durch die Auftragnehmerin erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt die Auftragnehmerin dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Änderungen des Verarbeitungsgegenstandes und Änderungen von Verarbeitungstätigkeiten sind gemeinsam zwischen Auftraggeber und Auftragnehmerin abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

3.3 Der Auftraggeber hat vor Beginn der Arbeiten sicherzustellen, dass der Auftragnehmerin personenbezogene Daten nur innerhalb der auftragsgemäß vereinbarten Leistungserbringung zukommen.

3.4 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. der Auftragnehmerin zu. Die Auftragnehmerin informiert den Auftraggeber unverzüglich, falls die Auftragnehmerin der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit die Auftragnehmerin anzweifelt, ist die Auftragnehmerin berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass die Auftragnehmerin durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden.

3.5 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine Weisung in Textform erfolgen konnte. Unabhängig von der Form der Erteilung dokumentieren sowohl die Auftragnehmerin als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrages und anschließend noch für drei Jahre aufzubewahren. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit – nach vorheriger Terminvereinbarung - regelmäßig im erforderlichen Umfang zu kontrollieren. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb der Auftragnehmerin nicht mehr als erforderlich beeinträchtigen. Die Ergebnisse der Kontrollen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

3.6 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsbefugnisse des Auftraggebers

4.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. der Auftragnehmerin zu. Die Auftragnehmerin informiert den Auftraggeber unverzüglich, falls die Auftragnehmerin der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit die Auftragnehmerin anzweifelt, ist die Auftragnehmerin berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass die Auftragnehmerin durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden.

4.2 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine Weisung in Textform erfolgen konnte. Unabhängig von der Form der Erteilung dokumentieren sowohl die Auftragnehmerin als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrages und anschließend noch für drei Jahre aufzubewahren.

4.3 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Die Auftragnehmerin legt Weisungsempfänger fest. Die weisungsberechtigten Personen sind **Anlage 3** dieses Vertrags zu entnehmen. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

5. Vertraulichkeit

5.1 Die Auftragnehmerin bestätigt, dass ihr die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Der Auftragnehmerin ist insbesondere bekannt, dass die Verschwiegenheitspflicht gemäß § 43a Abs. 2 BRAO, § 2 Berufsordnung der Rechtsanwälte (BORA) und § 18 BNotO über die in § 203 Strafgesetzbuch (StGB) geregelte allgemeine Schweigepflicht hinausgeht. Inhalt und Umfang der Verschwiegenheitsverpflichtung ergeben sich aus **Anlage 4** dieses Vertrags.

5.2 Die Auftragnehmerin wahrt bei der Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit. Diese Pflicht besteht auch nach Beendigung dieses Vertragsverhältnisses fort.

5.3 Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Die Auftragnehmerin verpflichtet diese Mitarbeiter durch schriftliche Vereinbarung für die Zeit der Tätigkeit und auch nach Beendigung des Beschäftigungsverhältnisses zur Wahrung der Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

5.4 Auskünfte an Dritte oder Betroffene darf die Auftragnehmerin nur nach vorheriger schriftlicher Zustimmung, oder Zustimmung in einem elektronischen Format, durch den Auftraggeber erteilen.

6. Technische und organisatorische Maßnahmen

Die Auftragnehmerin hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in **Anlage 1** dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung angepasst werden. Dabei müssen die

angepassten Maßnahmen mindestens dem Sicherheitsniveau der in der **Anlage 1** niedergelegten Maßnahmen entsprechen.

7. Unterstützungspflichten der Auftragnehmerin

Die Auftragnehmerin wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Auftragnehmerin wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die der Auftragnehmerin zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern

8.1 Die Auftragnehmerin ist zum Einsatz von Unterauftragsverarbeitern berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Unterauftragsverhältnisse der Auftragnehmerin sind abschließend diesem Vertrag in **Anlage 2** beigefügt.

8.2 Beabsichtigt die Auftragnehmerin den Einsatz weiterer Unterauftragsverarbeiter, wird die Auftragnehmerin dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des / der Unterauftragsverarbeiter(s) zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des / der Unterauftragsverarbeiter(s) als genehmigt. In dringenden Fällen (z.B. bei kurzfristig benötigten Fehleranalysen oder Mängelbeseitigungen), kann die Auftragnehmerin die Anzeige- und Widerspruchsfrist für Unterauftragsverarbeiter angemessen verkürzen. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragsverarbeiters die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und / oder sonstige berechtigte Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen. Erfolgt ein fristgerechter substantiierter Widerspruch, dürfen die betroffenen Unterauftragsverarbeiter nicht eingesetzt werden.

8.3 Hat der Auftraggeber Widerspruch gegen die Hinzuziehung eines Unterauftragsverarbeiters eingelegt ist die Auftragnehmerin berechtigt, den Hauptvertrag und diesen Auftragsverarbeitungsvertrag mit einer Frist von 4 Wochen zu kündigen.

8.4 Unterauftragsverarbeiter werden von der Auftragnehmerin unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragnehmerin und Unterauftragsverarbeiter müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Unterauftragsverarbeiters.

8.5 Eine Beauftragung von Unterauftragsverarbeitern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

8.6 Der Auftraggeber erteilt hiermit seine Zustimmung zur Beauftragung der in der **Anlage 2** aufgeführten Unterauftragsverarbeiter.

8.7 Die Auftragnehmerin stellt sicher, dass der Auftraggeber gegenüber dem Unterauftragsverarbeiter dieselben Weisungs- und Kontrollrechte wie gegenüber der Auftragnehmerin nach diesem Vertrag hat. Die Auftragnehmerin wird die Unterauftragsverarbeiter, die Zugriff auf Mandantendaten haben könnten, in Textform zur Verschwiegenheit verpflichten (§ 43 e Abs. 3 Nr. 3 BRAO).

9. Informationspflichten der Auftragnehmerin

9.1 Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt

bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß von der Auftragnehmerin selbst, einer bei der Auftragnehmerin angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die die Auftragnehmerin zur Erfüllung vertraglicher Pflichten eingesetzt hat, begangen wurde.

9.2 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter die Auftragnehmerin um Auskunft, Berichtigung oder Löschung von Daten, die Justin LegalTech GmbH als Auftragsverarbeiter verarbeitet, wird die Auftragnehmerin die Anfrage unverzüglich an den Auftraggeber weiterleiten und das weitere Vorgehen mit ihm abstimmen.

9.3 Die Auftragnehmerin wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von denen auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat die Auftragnehmerin den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Der Auftragsverarbeitungsvertrag gilt nach Beendigung des Hauptvertrags für 3 Monate fort. Sollte in diesem Zeitraum eine Reaktivierung des Accounts erfolgen und der Hauptvertrag damit weitergeführt werden, gilt der Auftragsverarbeitungsvertrag wieder wie zuvor. Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung des Hauptvertrags hat die Auftragnehmerin alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine rechtliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen).

Die Rückgabe der Daten erfolgt entweder durch eigenständige Sicherung der Daten durch den Auftraggeber oder durch Übersendung der Daten in einem maschinenlesbaren Format über ein Datennetz. Die Übersendung der Daten stellt eine zusätzliche Unterstützungsleistung dar, für die die Auftragnehmerin eine angemessene Vergütung verlangen darf.

Die Auftragnehmerin wird sämtliche auf ihren Servern verbleibende Daten des Auftraggebers vorbehaltlich vorrangiger nationaler oder unionsrechtlicher Speicherpflichten 90 Tage nach Beendigung des Hauptvertrags löschen, es sei denn der Auftraggeber wünscht eine frühere Löschung.

11. Schlussbestimmungen

11.1 Es gilt das Recht des Bundesrepublik Deutschland. Gerichtsstand für alle Streitigkeiten ist das für den Sitz der Auftragnehmerin örtlich zuständige Gericht, sofern beide Vertragsparteien Kaufmann oder juristische Personen des öffentlichen Rechts sind oder keinen allgemeinen Gerichtsstand in Deutschland besitzen.

11.2 Soweit die Verarbeitung personenbezogener Daten im Auftrag betroffen ist, gehen die Regelungen dieses Vertragsgegenüber den Regelungen der Hauptvereinbarung vor.

11.3 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

11.4 Die Auftragnehmerin ist berechtigt, die vorliegenden Regelungen aus sachlich gerechtfertigten Gründen (z.B. Änderungen in der Rechtsprechung, Gesetzeslage, Marktgegebenheiten oder der Geschäfts- oder Unternehmensstrategie) und unter Einhaltung einer angemessenen Frist zu ändern. Bestandskunden werden hierüber spätestens zwei Wochen vor Inkrafttreten der Änderung per E-Mail benachrichtigt. Sofern der Bestandskunde nicht innerhalb der in der Änderungsmitteilung gesetzten Frist widerspricht, gilt seine Zustimmung zur Änderung als erteilt. Im Falle des Widerspruchs ist die Auftragnehmerin berechtigt, den Vertrag zum Zeitpunkt des Inkrafttretens der Änderung außerordentlich zu kündigen. Die Benachrichtigung über die beabsichtigte Änderung dieser

Nutzungsbedingungen wird auf die Frist und die Folgen des Widerspruchs oder seines Ausbleibens hinweisen.

11.5 Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht. Die Vertragsparteien werden sich bemühen, anstelle der unwirksamen Bestimmungen eine solche zu finden, die dem Vertragsziel rechtlich und wirtschaftlich am ehesten gerecht wird. Das gleiche gilt entsprechend für den Fall einer Vertragslücke.

Berlin,

Lukas Pagel
(Geschäftsführer)

Anlagen:

Nr.	Bezeichnung
Anlage 1	Technische und organisatorische Maßnahmen
Anlage 2	Unterauftragsverarbeiter
Anlage 3	Weisungsberechtigte
Anlage 4	Verschwiegenheitsverpflichtung
Anlage 4a	Vorschriften zur anwaltlichen Verschwiegenheit

Anlage 1 – Technische und organisatorischen Maßnahmen der Auftragnehmerin nach Art. 32 DSGVO

Justin LegalTech GmbH setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um.

I. Zutrittskontrolle

Die Gebäude am Standort der Auftragnehmerin, in dem sich die Räumlichkeiten der Auftragnehmerin befinden und von denen die Auftragnehmerin in der Regel die Dienstleistungen erbringt, verfügen meist über einen Haupt- sowie mehrere Notausgänge. Über die Notausgänge besteht von außen kein Zutritt. Mitarbeiter sind angewiesen, die Räumlichkeiten nur über den Hauptausgang zu verlassen.
Die Räumlichkeiten der Auftragnehmerin sind durch eine Zutrittskontrolle (Schließanlage) mittels eines Smart Locks geschützt. Zugänge via Smart Lock werden nur an Berechtigte ausgegeben.
Es existiert ein dokumentiertes Verfahren für die Vergabe und den Entzug von Zutrittsrechten, welche durch die Verwaltungsabteilung gewährt wird.
Die Räumlichkeiten verfügen größtenteils über eine Alarmanlage. Am Hauptstandort verfügen die Räumlichkeiten über Bewegungsmelder. Sollte ein Alarm ausgelöst werden, geht die Meldung direkt bei einer Sicherheitsfirma ein, die die Sicherheitstechnik betreut.
Besucher an allen Standorten werden nach Identifikation durch Mitarbeiter der Verwaltung in das Gebäude gelassen. Anschließend warten sie in einem Besucherbereich, bis sie vom Besuchten abgeholt werden.
Die Mitarbeiter der Auftragnehmerin sind angewiesen, mobile Geräte stets beaufsichtigt oder verschlossen zu halten und bei längeren Fehlzeiten zur sicheren Aufbewahrung an die IT zu übergeben.
Bevor Mitarbeiter der Auftragnehmerin am mobilen Arbeitsplatz tätig sind, werden sie von der Auftragnehmerin zusätzlich zu den allgemein geltenden betrieblichen Bestimmungen zu Datenschutz und Datensicherheit durch eine Richtlinie „Mobiles Arbeiten“ verpflichtet. Die darin enthaltenen Regelungen beinhalten u.a. den Umgang mit Daten, Sicherheitsmaßnahmen am mobilen Arbeitsplatz, rechtliche Folgen bei Verstößen und Beendigung der Nutzung des mobilen Arbeitsplatzes. Die Auftragnehmerin hält eine aktuelle Liste der mit mobilen Endgeräten ausgestatteten und im Rahmen des Auftrags tätigen Mitarbeiter nach.

Azure Cloud

Die eingesetzte IT Infrastruktur wird vollständig auf ISO 27001-zertifizierten in Europa befindlichen Microsoft Azure Servern gehostet und betrieben. Microsoft beschränkt den Zugang zu Einrichtungen, in denen sich Informationssysteme befinden, die Kundendaten oder Professional Services-Daten verarbeiten, auf identifizierte, autorisierte Personen.
Folgende Quellen bieten Ihnen umfangreiche weitere Informationen zu den implementierten Maßnahmen seitens Microsoft:
https://learn.microsoft.com/de-de/azure/security/fundamentals/physical-security
https://azure.microsoft.com/de-de/explore/trusted-cloud/
https://docs.microsoft.com/de-de/azure/compliance/

II. Zugangs- und Zugriffskontrolle

Mitarbeiter der Auftragnehmerin sind mittels einer Vereinbarung zum vertrauensvollen Umgang mit Daten verpflichtet worden. Dies umfasst auch den vertrauensvollen Umgang mit Passwörtern.
Die Mitarbeiter sind angehalten Ihre Bildschirme bei Abwesenheit zu sperren. Die Laptops sind nach Beendigung der Arbeit in den Räumlichkeiten der Auftragnehmerin von den Mitarbeitern in gesicherten Schränken einzuschließen, sofern sie nicht an einem mobilen Arbeitsplatz genutzt werden.
Jeder Rechner verfügt über eine aktuelle Antivirensoftware und eine Software-Firewall.
Durch ein Berechtigungskonzept wird sichergestellt, dass Mitarbeiter der Auftragnehmerin nur auf Programme und Daten zugreifen können, die sie zur Aufgabenerfüllung benötigen (Need-to-know-Prinzip). Zusätzlich werden die Anwendungen über eine Username-/Passwort-Authentifizierung sowie eine zusätzliche Multi-Faktor-Authentifizierung geschützt.
Der Umgang mit den Accounts und der IT-Infrastruktur sowie der sichere Umgang mit Passwörtern (Mindestlänge, etc.) ist in konkreten Arbeitsanweisungen für die Mitarbeiter geregelt. Die Weitergabe von persönlichen Zugangsdaten oder –mitteln ist untersagt.

Azure Cloud

Der Zugriff auf die in Microsoft Azure betriebene Infrastruktur ist nur über gesicherte Wege sowie Multi-Faktor-Authentifizierung und von bestimmten IP Adressen aus möglich.
Des Weiteren führt Microsoft Aufzeichnungen über die ein- und ausgehenden Medien, die Kundendaten oder Professional Services-Daten enthalten, einschließlich der Art der Medien, des zugelassenen Absenders/Empfängers, des Datums und der Uhrzeit, der Anzahl der Medien und der darin enthaltenen Arten von solchen Daten.
Folgende Quellen bieten Ihnen umfangreiche weitere Informationen zu den implementierten Maßnahmen seitens Microsoft:
https://www.microsoft.com/de-de/trust-center
https://azure.microsoft.com/de-de/explore/trusted-cloud/
https://docs.microsoft.com/de-de/azure/compliance/

III. Eingabekontrolle

Es sind Protokollierungen der Aktivitäten des IT-Systems selbst (Protokolle der Aktivitäten des Anti-Viren-Systems und/oder der Firewall) eingerichtet. Darüber hinaus sind Protokollierungsmaßnahmen bezüglich der Aktivitäten der IT-Administratoren und der Benutzer selbst eingerichtet. Die Verwendung mobiler Datenträger ist untersagt.

IV. Auftragskontrolle

Die Auftragnehmerin verarbeitet personenbezogene Daten des Auftraggebers ausschließlich im vertraglich festgelegten Rahmen sowie auf Weisung des Auftraggebers.
Hierbei setzt die Auftragnehmerin auch die in Anlage 2 aufgeführten Unterauftragsverarbeiter ein.
Im Falle eines Auftragsverarbeitungsverhältnisses hat die Auftragnehmerin mit dem jeweiligen Vertragspartner einen Auftragsverarbeitungsvertrag abgeschlossen, der zwingend den gem. Art. 28 Abs. 3 DSGVO erforderlichen Regelungsgehalt aufweist. Unterauftragnehmer der Auftragnehmerin erhalten nur Zugriff auf die Systeme des Auftraggebers, sofern der Auftraggeber vorab diesen Zugriff selbst gewährt bzw. durch die Auftragnehmerin gewähren lässt. Sie werden regelmäßig zur Vorlage aktueller Prüfnachweise bezüglich ihrer vertraglichen Pflichten aufgefordert und im Fall der Verarbeitung von Mandantendaten von der Auftragnehmerin zusätzlich zur Verschwiegenheit verpflichtet, § 43e Abs. 3 BRAO / § 26a Abs. 3 BNotO.
Die Auftragnehmerin arbeitet nur mit (Unter-)Auftragnehmern zusammen, die die Sicherheit der personenbezogenen Daten garantieren können. Dies bemisst sich nach den von dem jeweiligen Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen.

Azure und Azure OpenAI Services (u.a. ChatGPT)

Die Nutzung von ChatGPT erfolgt als Teil des Services von Microsoft Azure. Wir verfügen über eine eigene Azure OpenAI-Instanz, die u.a. das ChatGPT-Modell beinhaltet, welche nicht der öffentlich verfügbaren Ressource von OpenAI entspricht. Mit dem Dienstleister wurden sämtliche verfügbaren zusätzlichen Abkommen und datenschutzfreundlichen Einstellungsmöglichkeiten getroffen, um unter anderem auch das Mitlesen und den Missbrauch der verarbeiteten Daten zu verhindern. Da wir den Service mit modifiziertem Content Filter nutzen und die Missbrauchsüberwachung deaktiviert haben, speichert Microsoft hierfür keine Anfragen und Ausfüllungen. Die betroffenen Daten werden außerdem ausdrücklich nicht zum Anlernen der Microsoft KI verwendet. Zur bestmöglichen Vorbeugung gegen eine mögliche Halluzination wurden entsprechende Einstellungen hinsichtlich der Kreativität gewählt.
Folgende Quellen bieten Ihnen umfangreiche weitere Informationen zu den implementierten Maßnahmen bezüglich Microsoft als (Unter-)Auftragsverarbeiter und Azure OpenAI:
https://learn.microsoft.com/de-de/legal/cognitive-services/openai/data-privacy
https://learn.microsoft.com/de-de/legal/cognitive-services/openai/limited-access
AVV Microsoft: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

V. Datentrennungs- und Weitergabekontrolle

Daten, die verschiedene Kunden/Auftraggeber betreffen und Daten die zu verschiedenen Zwecken verarbeitet werden sind in geeigneter Weise durch kundenspezifische Ordner sowie Accounts und durch geeignete kundenspezifische Verschlüsselungs-Maßnahmen auf Anwendungsebene voneinander getrennt.
Die Auftragnehmerin entwickelt überdies in einer lokalen Umgebung und testet im Anschluss auf dedizierten

Development- und Staging-Umgebungen. Erst im Anschluss und nach dem Bestehen aller Qualitäts- und Sicherheitschecks wird an das separate Produktiv-System ausgeliefert.

WLAN-Zugänge sind mit dem WPA2-Standard gesichert. Für Besucher gibt es einen eigenen WLAN-Zugang, der nicht mit dem restlichen IT-System des Unternehmens verbunden ist. Zudem werden die WLAN-Authentifizierungen in regelmäßigen Abständen mit Hilfe der Log-Dateien Authentifizierung kontrolliert. Die Übertragung von Daten auf dem elektronischen Weg wird an diversen Stellen durch in Summe mehrere dutzend Verschlüsselungstechniken und -algorithmen (unter anderem – aber nicht abschließend – SSL, TSL, AES) gesichert.

VI. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Verfügbarkeit und Belastbarkeit

Bei der Entwicklung von Verarbeitungsvorgängen werden geeignete technische Maßnahmen implementiert, um die geplanten Verarbeitungsvorgänge datenschutzkonform zu gestalten. Des Weiteren werden beispielsweise durch entsprechende Voreinstellungen, bei denen die Software nur die nötigsten Daten sammelt, Maßnahmen getroffen, um die Anforderung Privacy by Default einzuhalten.

Eine Sicherung der (elektronischen) Daten erfolgt täglich. Darüber hinaus existiert ein Notfallplan mit Alarmierungs- und Wiederanlaufplan im Falle eines Ausfalls der IT. Der IT-Betrieb wird durch diverse Diagnostiktools überwacht, die bei einer Störung oder einem Ausfall automatisch den IT-Sicherheitsbeauftragten / die IT-Administratoren benachrichtigen.

VII. Organisation und Wirksamkeitskontrolle

Die Mitarbeiter sind zur Wahrung der Vertraulichkeit hinsichtlich personenbezogener Daten verpflichtet und werden regelmäßig im Datenschutz geschult.

Es erfolgen regelmäßige Kontrollen der Wirksamkeit der eingesetzten technischen und organisatorischen Maßnahmen. Unter anderem – aber nicht abschließend – wird hierzu regelmäßig die Funktionstüchtigkeit der Anti-Viren-Softwares und der Firewalls überprüft und kontrolliert, ob die den Mitarbeitern erteilten Berechtigungen noch deren Aufgaben und Positionen entsprechen. Darüber hinaus werden regelmäßig Penetrationstests sowie interne Audits durchgeführt.

Anlage 2 – Liste der bestehenden Unterauftragsverarbeiter

(Unternehmens-) Name und Anschrift	Beschreibung der Leistung	Verarbeitung von Mandantendaten	Land der Leistungserbringung
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Der Dienstleister stellt die Cloud-Lösung „Microsoft Azure“ bereit, auf der die vertragsgegenständliche SaaS-Lösung gehostet wird.	Ja	Deutschland / EU
Sendinblue GmbH, Köpenicker Straße 126, 10179 Berlin	Der Dienstleister stellt eine Lösung zum transaktionalen Versandt von E-Mails bereit, die von der die vertragsgegenständliche SaaS-Lösung genutzt wird.	Nein	Deutschland / EU
Zoho Corporation GmbH, Trinkausstr. 7, 40213 Düsseldorf	Der Dienstleister stellt eine Lösung für Support- und Ticketsysteme bereit, die von der vertragsgegenständlichen SaaS-Lösung genutzt wird.	Nein	Deutschland / EU
Calendly, LLC, 1315 Peachtree St NE, Atlanta, GA 30309, USA	Der Dienstleister stellt eine Lösung zur Terminabstimmung bereit.	Nein	USA

Anmerkungen:
Im Fall der Verarbeitung von Mandantendaten durch einen Unterauftragsverarbeiter wurde dieser vor einer entsprechenden Datenverarbeitung von der Auftragnehmerin zusätzlich zur Verschwiegenheit verpflichtet, § 43e Abs. 3 BRAO / § 26a Abs. 3 BNotO.

Die Nutzung von ChatGPT erfolgt als Teil des Services von Microsoft Azure und entspricht nicht der öffentlich verfügbaren Ressource. Mit dem Dienstleister wurden sämtliche verfügbaren zusätzlichen Abkommen und Einstellungsmöglichkeiten getroffen, um das Mitlesen und den Missbrauch der verarbeiteten Daten zu verhindern. Da wir den Service mit modifiziertem Content Filter nutzen und die Missbrauchsüberwachung deaktiviert haben, speichert Microsoft hierfür keine Anfragen und Ausfüllungen. Die betroffenen Daten werden außerdem ausdrücklich nicht zum Anlernen der Microsoft KI verwendet. Zur Vorbeugung gegen eine mögliche Halluzination wurden zudem entsprechende Einstellungen hinsichtlich der Kreativität gewählt.

Die Auftragnehmerin weist darauf hin, dass Anfragen des Auftraggebers über das Ticketsystem keine personenbezogenen Mandantendaten beinhalten dürfen.

Anlage 3 - Weisungsberechtigte

Berechtigte Weisungsgeber:
Zur Erteilung von Weisungen betreffend die Auftragsverarbeitung ist ausschließlich der Auftraggeber berechtigt.

Berechtigte Weisungsempfänger:

Lukas Pagel
Geschäftsführer
030 – 285 05 928
lukas.pagel@justin-legal.com

André Floß
Lead Sales & Marketing
030 – 24537107
andre.floss@justin-legal.com

Anlage 4 – Verschwiegenheitsverpflichtung

Verschwiegenheitsverpflichtung nach § 43e Absatz 3 Nummer 1 Bundesrechtsanwaltsordnung (BRAO)

Die Justin LegalTech GmbH, Saarbrücker Str. 18 10405 Berlin verpflichtet sich bei der Bereitstellung der SaaS-Software-Produkte gegenüber seinem Kunden in folgender Weise zur Verschwiegenheit im Sinne des § 43e Abs. 3 Nr. 1 BRAO:

Die Justin LegalTech GmbH ist über den Umfang ihrer Verschwiegenheitspflicht bei der Bereitstellung der SaaS-Software-Produkte gegenüber Rechtsanwälten und deren Hilfspersonen in Kenntnis gesetzt worden. Der Justin LegalTech GmbH sind die auf den Folgeseiten abgedruckten Bestimmungen bekannt. Der Justin LegalTech GmbH ist insbesondere bekannt, dass die Verschwiegenheitspflicht gemäß §§ 43a Abs. 2 und 43e Bundesrechtsanwaltsordnung und § 2 Berufsordnung der Rechtsanwälte über die in § 203 Strafgesetzbuch geregelte allgemeine Schweigepflicht hinausgeht. Die Justin LegalTech GmbH verpflichtet sich ausdrücklich, auch insoweit Verschwiegenheit zu wahren.

Der Justin LegalTech GmbH ist bekannt, dass

1. sich ihre Verschwiegenheitspflicht nicht nur auf fremde Geheimnisse erstreckt, sondern auf alle Tatsachen, die der Justin LegalTech GmbH in Ausübung oder aus Anlass ihrer Tätigkeit anvertraut oder bekannt werden, so auch schon die Tatsache, dass dem Rechtsanwalt ein bestimmtes Mandat erteilt worden ist oder die Anbahnung eines bestimmten Mandats ansteht;
2. sich die Verschwiegenheitspflicht auch erstreckt auf die internen Büroverhältnisse sowie die der Justin LegalTech GmbH bei ihrer Tätigkeit bekanntwerdenden persönlichen, wirtschaftlichen und steuerlichen Verhältnisse des Rechtsanwalts und der anderen Mitarbeiter;
3. die Verschwiegenheitspflicht gegenüber jedermann besteht, so auch gegenüber Familienangehörigen, gegenüber Arbeitskollegen, soweit eine Mitteilung nicht aus dienstlichen Gründen erfolgt, gegenüber demjenigen, der von der betreffenden Tatsache bereits Kenntnis erlangt hat;
4. die Verschwiegenheitspflicht auch nach Beendigung der Vertragsbeziehung fortbesteht.

Die gesetzlichen Bestimmungen zum Zeugnisverweigerungsrecht (vgl. Anlage 4a) sind der Justin LegalTech GmbH ebenfalls bekannt. Die Justin LegalTech GmbH wird bei Gerichten und Behörden über Tatsachen, die ihr bei ihrer Tätigkeit bekannt werden, ohne vorherige Genehmigung des Rechtsanwalts nicht aussagen oder sonst Auskunft erteilen.

Anlage 4a - Vorschriften zur anwaltlichen Verschwiegenheit

I. Verschwiegenheitspflicht

§ 43a Abs. 2 Bundesrechtsanwaltsordnung

(2) Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm in Ausübung seines Berufes bekanntgeworden ist. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Rechtsanwalt hat die von ihm beschäftigten Personen in schriftlicher Form zur Verschwiegenheit zu verpflichten und sie dabei über die strafrechtlichen Folgen einer Pflichtverletzung zu belehren. Zudem hat er bei ihnen in geeigneter Weise auf die Einhaltung der Verschwiegenheitspflicht hinzuwirken. Den von dem Rechtsanwalt beschäftigten Personen stehen die Personen gleich, die im Rahmen einer berufsvorbereitenden Tätigkeit oder einer sonstigen Hilfstätigkeit an seiner beruflichen Tätigkeit mitwirken. Satz 4 gilt nicht für Referendare und angestellte Personen, die im Hinblick auf die Verschwiegenheitspflicht den gleichen Anforderungen wie der Rechtsanwalt unterliegen. Hat sich ein Rechtsanwalt mit anderen Personen, die im Hinblick auf die Verschwiegenheitspflicht den gleichen Anforderungen unterliegen wie er, zur gemeinschaftlichen Berufsausübung zusammengeschlossen und besteht zu den Beschäftigten ein einheitliches Beschäftigungsverhältnis, so genügt auch der Nachweis, dass eine andere dieser Personen die Verpflichtung nach Satz 4 vorgenommen hat.

§ 43e Bundesrechtsanwaltsordnung
(1) Der Rechtsanwalt darf Dienstleistern den Zugang zu Tatsachen eröffnen, auf die sich die Verpflichtung zur Verschwiegenheit gemäß § 43a Absatz 2 Satz 1 bezieht, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Dienstleister ist eine andere Person oder Stelle, die vom Rechtsanwalt im Rahmen seiner Berufsausübung mit Dienstleistungen beauftragt wird.
(2) Der Rechtsanwalt ist verpflichtet, den Dienstleister sorgfältig auszuwählen. Er hat die Zusammenarbeit unverzüglich zu beenden, wenn die Einhaltung der dem Dienstleister gemäß Absatz 3 zu machenden Vorgaben nicht gewährleistet ist.
(3) Der Vertrag mit dem Dienstleister bedarf der Textform. In ihm ist
1. der Dienstleister unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten,
2. der Dienstleister zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und
3. festzulegen, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.
(4) Bei der Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, darf der Rechtsanwalt dem Dienstleister den Zugang zu fremden Geheimnissen unbeschadet der übrigen Voraussetzungen dieser Vorschrift nur dann eröffnen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet.
(5) Bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, darf der Rechtsanwalt dem Dienstleister den Zugang zu fremden Geheimnissen nur dann eröffnen, wenn der Mandant darin eingewilligt hat.
(6) Die Absätze 2 und 3 gelten auch im Fall der Inanspruchnahme von Dienstleistungen, in die der Mandant eingewilligt hat, sofern der Mandant nicht ausdrücklich auf die Einhaltung der in den Absätzen 2 und 3 genannten Anforderungen verzichtet hat.
(7) Die Absätze 1 bis 6 gelten nicht, soweit Dienstleistungen auf Grund besonderer gesetzlicher Vorschriften in Anspruch genommen werden. Absatz 3 Satz 2 gilt nicht, soweit der Dienstleister hinsichtlich der zu erbringenden Dienstleistung gesetzlich zur Verschwiegenheit verpflichtet ist.
(8) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.

II. Berufsordnung der Rechtsanwälte

§ 2 Verschwiegenheit

(1) Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet und berechtigt. 2Dies gilt auch nach Beendigung des Mandats.
(2) Die Verschwiegenheitspflicht gebietet es dem Rechtsanwalt, die zum Schutze des Mandatsgeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, die risikoadäquat und für den Anwaltsberuf zumutbar sind. Technische Maßnahmen sind hierzu ausreichend, soweit sie im Falle der Anwendbarkeit der Vorschriften zum Schutz personenbezogener Daten deren Anforderungen entsprechen. Sonstige technische Maßnahmen müssen ebenfalls dem Stand der Technik entsprechen. Abs. 4 lit. c) bleibt hiervon unberührt.
Zwischen Rechtsanwalt und Mandant ist die Nutzung eines elektronischen oder sonstigen Kommunikationsweges, der mit Risiken für die Vertraulichkeit dieser Kommunikation verbunden ist, jedenfalls dann erlaubt, wenn der Mandant ihr zustimmt. Von einer Zustimmung ist auszugehen, wenn der Mandant diesen Kommunikationsweg vorschlägt oder beginnt und ihn, nachdem der Rechtsanwalt zumindest pauschal und ohne technische Details auf die Risiken hingewiesen hat, fortsetzt.
(3) Ein Verstoß gegen die Pflicht zur Verschwiegenheit (§ 43a Abs. 2 Bundesrechtsanwaltsordnung) liegt nicht vor, soweit Gesetz und Recht eine Ausnahme fordern oder zulassen.
(4) Ein Verstoß ist nicht gegeben, soweit das Verhalten des Rechtsanwalts
a) mit Einwilligung erfolgt oder
b) zur Wahrnehmung berechtigter Interessen erforderlich ist, z.B. zur Durchsetzung oder Abwehr von Ansprüchen aus dem Mandatsverhältnis oder zur Verteidigung in eigener Sache, oder
c) im Rahmen der Arbeitsabläufe der Kanzlei, die außerhalb des Anwendungsbereichs des § 43e Bundesrechtsanwaltsordnung liegen, objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz).
(5) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.

III. Strafbarkeit der Verletzung von Privatgeheimnissen

§ 203 Strafgesetzbuch (Auszug)

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle
anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.
(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Datenschutzbeauftragter bekannt geworden ist. Ebenso wird bestraft, wer
1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.
(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.
(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

IV. Zeugnisverweigerungsrecht

§ 53 Strafprozessordnung (Auszug)

(1) Zur Verweigerung des Zeugnisses sind ferner berechtigt
3.Rechtsanwälte und Kammerrechtsbeistände, Patent-anwälte, Notare, Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater und Steuerbevollmächtigte, Ärzte, Zahnärzte, Psychotherapeuten, Psychologische Psychotherapeuten, Kinder- und Jugendlichen-psychotherapeuten, Apotheker und Hebammen über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist; für Syndikusrechtsanwälte (§ 46 Absatz 2 der Bundesrechtsanwaltsordnung) und Syndikus-patentanwälte (§ 41a Absatz 2 der Patentanwaltsordnung) gilt dies vorbehaltlich des § 53a nicht hinsichtlich dessen, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist;
(2) Die in Absatz 1 Satz 1 Nr. 2 bis 3b Genannten dürfen das Zeugnis nicht verweigern, wenn sie von der Verpflichtung zur Verschwiegenheit entbunden sind.

§ 53a Strafprozessordnung

(1) Den Berufsgeheimnisträgern nach § 53 Absatz 1 Satz 1 Nummer 1 bis 4 stehen die Personen gleich, die im Rahmen
1. eines Vertragsverhältnisses,
2. einer berufsvorbereitenden Tätigkeit oder
3. einer sonstigen Hilfstätigkeit
an deren beruflicher Tätigkeit mitwirken. Über die Ausübung des Rechts dieser Personen, das Zeugnis zu verweigern, entscheiden die Berufsgeheimnisträger, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann.
(2) Die Entbindung von der Verpflichtung zur Verschwiegenheit (§ 53 Absatz 2 Satz 1) gilt auch für die nach Absatz 1 mitwirkenden Personen.

§ 20c Bundeskriminalamtgesetz (Auszug)

(3) Unter den in den §§ 52 bis 55 der Strafprozessordnung bezeichneten Voraussetzungen ist der Betroffene zur Verweigerung der Auskunft berechtigt. Dies gilt nicht, soweit die Auskunft zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person erforderlich ist. Eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder 4 der Strafprozessordnung genannte Person ist auch in den Fällen des Satzes 2 zur Verweigerung der Auskunft berechtigt. Die betroffene Person ist über ihr Recht zur Verweigerung der Auskunft zu belehren. Auskünfte, die gemäß Satz 2 erlangt wurden, dürfen nur für den dort bezeichneten Zweck verwendet werden.

Den Bestimmungen der Strafprozessordnung entspricht – in anderer sprachlicher Fassung – die Regelung für den Zivilprozess:

§ 383 Zivilprozessordung (Auszug)

(1) Zur Verweigerung des Zeugnisses sind berechtigt:
6. Personen, denen kraft ihres Amtes, Standes oder Gewerbes Tatsachen anvertraut sind, deren Geheimhaltung durch ihre Natur oder durch gesetzliche Vorschrift geboten ist, in Betreff der Tatsachen, auf welche die Verpflichtung zur Verschwiegenheit sich bezieht.

(3) Die Vernehmung der unter Nummern 4 bis 6 bezeichneten Personen ist, auch wenn das Zeugnis nicht verweigert wird, auf Tatsachen nicht zu richten, in Ansehung welcher erhellt, dass ohne Verletzung der Verpflichtung zur Verschwiegenheit ein Zeugnis nicht abgelegt werden kann.

§ 385 Abs. 2 Zivilprozessordnung
(2) Die im § 383 Nr. 4, 6 bezeichneten Personen dürfen das Zeugnis nicht verweigern, wenn sie von der Verpflichtung zur Verschwiegenheit entbunden sind.

Das Zeugnisverweigerungsrecht ist für die anderen Gerichtszweige und auch für Verwaltungsverfahren genauso wie für den Zivilprozess und den Strafprozess geregelt.

Vergleiche:

- § 29 Abs. 2 Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit
- §§ 46 Abs. 2, 80 Abs. 2 Arbeitsgerichtsgesetz
- § 98 Verwaltungsgerichtsordnung
- § 118 Abs. 1 Sozialgerichtsgesetz
- § 84 Abs. 1 Finanzgerichtsordnung
- § 28 Abs. 1 Bundesverfassungsgerichtsgesetz
- § 65 Abs. 1 Verwaltungsverfahrensgesetz
- § 102 Abgabenordnung