

Auftragsverarbeitungsvereinbarung gemäß Art. 28 DSGVO („AVV“)

zwischen

Formivio UG (haftungsbeschränkt)

vertreten durch den Geschäftsführer Moritz Neudel

Steinwiesenweg 12

86938 Schondorf am Ammersee

HRB 42875, Amtsgericht Augsburg

– Auftragsverarbeiter – nachfolgend „Auftragnehmer“ genannt –
und

[Name der Steuerkanzlei / Steuerberatungsgesellschaft]

[Straße und Hausnummer]

[PLZ und Ort]

– Verantwortlicher – nachfolgend „Auftraggeber“ genannt –
– nachfolgend einzeln jeweils auch „Partei/en“ genannt –

Präambel

Diese Vereinbarung legt die Rechte und Pflichten des Auftragnehmers und des Auftraggebers im Rahmen der Verarbeitung von personenbezogenen Daten im Auftrag gemäß Art. 28 der EU-Datenschutzgrundverordnung („DSGVO“) fest. Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

§ 1 Gegenstand und Dauer der Verarbeitung

- (1) Der Gegenstand der Verarbeitung ergibt sich aus dem Vertrag „Nutzungsvereinbarung Postfachpilot“, auf den im Folgenden verwiesen wird (nachfolgend „Hauptvertrag“ genannt).
- (2) Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Hauptvertrags.
- (3) Soweit die Laufzeit des Hauptvertrags beendet sein sollte, gilt diese Vereinbarung unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

§ 2 Art der Daten und Zweck der Verarbeitung

- (1) Der Auftragnehmer erbringt für den Auftraggeber die Leistungen gemäß des Hauptvertrags, insbesondere die KI-gestützte Vorverarbeitung des E-Mail-Eingangs (automatische Klassifizierung, Extraktion relevanter Informationen sowie Erstellung von Antwort- und Schreibentwürfen) und die Unterstützung bei der Fristenüberwachung. Darüber hinaus erbringt er Wartungs- und Supportleistungen für den Auftraggeber, wodurch die Möglichkeit des Zugriffs auf die nachstehend genannten Arten personenbezogener Daten besteht, die mit der Software verarbeitet oder auf dem zur Verfügung gestellten Speicherplatz gespeichert werden.
- (2) Gegenstand der Verarbeitung personenbezogener Daten können dabei die folgenden Datenarten/-kategorien sein:
 - allgemeine Personendaten (Name, Geburtsdatum, Geburtsort, Staatsangehörigkeit)
 - Kommunikationsdaten (Anschrift, Telefonnummer, E-Mail)
 - Steuer- und Finanzdaten (z. B. Steuernummer, Steuer-ID, Einkünfte, Buchhaltungs- und Belegdaten)
 - Zahlungsdaten (Bankverbindung)
 - besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO, insbesondere Gesundheitsdaten i. S. d. Art. 4 Nr. 15 DSGVO, soweit sich aus den verarbeiteten

Unterlagen Informationen über den Gesundheitszustand einer Person ableiten lassen (z. B. Krankheitskosten als außergewöhnliche Belastungen)

- Sozialdaten i. S. d. § 67 Abs. 2 SGB X (z. B. aus Lohn- und Gehaltsabrechnung sowie Sozialversicherung), soweit diese im Rahmen des Mandats verarbeitet werden

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen die folgenden:

- Beschäftigte des Auftraggebers
- Mandanten und Kunden des Auftraggebers
- an den Leistungen des Auftraggebers Interessierte

§ 3 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer versichert, dass ihm die einschlägigen, geltenden Datenschutzvorschriften bekannt sind und er jederzeit die Grundsätze zur ordnungsgemäßen Verarbeitung personenbezogener Daten beachtet. Diese Vereinbarung entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.
- (2) Der Auftragnehmer verarbeitet personenbezogene Daten grundsätzlich nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn, er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Die anfänglichen Weisungen des Auftraggebers werden durch diese Vereinbarung und den Hauptvertrag festgelegt. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Meinung ist, eine Weisung verstoße gegen geltende Datenschutzvorschriften.
- (3) Der Auftragnehmer wird die Daten für keine anderen als die festgelegten Zwecke verwenden.
- (4) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung der Daten die Vertraulichkeit zu wahren und setzt bei der Erbringung seiner Leistungen nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
- (5) Soweit der Auftraggeber als Berufsgeheimnisträger einer gesetzlichen Geheimhaltungspflicht gem. § 203 StGB unterliegt und der Auftragnehmer im Rahmen dieser Vereinbarung Kenntnis von Daten oder Informationen erlangt, die dem Schutzbereich dieser Verschwiegenheitspflicht unterliegen, verpflichtet sich der Auftragnehmer entsprechend zur Verschwiegenheit nach § 203 Abs. 4 StGB. Soweit darüber hinaus Sozialdaten verarbeitet werden, die dem Sozialgeheimnis (§ 35 SGB I, § 78 SGB X) unterliegen, verpflichtet sich der Auftragnehmer auch insoweit zur Wahrung der Vertraulichkeit. Die Einzelheiten der Verpflichtungserklärung ergeben sich aus **Anhang 1** zu dieser Vereinbarung.
- (6) Die Parteien arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- (7) Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diese Vereinbarung und die Verarbeitung der Daten des Auftraggebers beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten nach dieser Vereinbarung beim Auftragnehmer ermittelt.
- (8) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technisch-organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen sichergestellt ist.
- (9) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Kenntnisnahme an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere gem. Art. 33, 34 DSGVO nachkommen kann. Er wird über den gesamten Vorgang eine Dokumentation erstellen, die er dem Auftraggeber auf Nachfrage zur Kenntnisnahme und für weitere Maßnahmen übermittelt.
- (10) Der Auftragnehmer verpflichtet sich, den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden

und Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen zur Verfügung zu stellen.

- (11) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, wird der Auftragnehmer den Auftraggeber auf dessen Kosten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen. Dies gilt gleichermaßen für eine ggf. bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde. Die Parteien werden sich über die Modalitäten und Konditionen im Einzelfall schriftlich oder in Textform verständigen.

§ 4 Technisch-organisatorische Maßnahmen („TOMs“)

- (1) Der Auftragnehmer verpflichtet sich, in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorischen Maßnahmen gem. Art. 32 DSGVO zum Schutze der personenbezogenen Daten zu ergreifen, die im Auftrag des Auftraggebers verarbeitet werden. Die Dokumentation der technisch-organisatorischen Maßnahmen wird zum Zeitpunkt des Vertragsschlusses in **Anhang 2** verbindlich zwischen den Parteien festgelegt.
- (2) Die in Anhang 2 dargestellten technisch-organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, entsprechend angepasste Maßnahmen in Zukunft umzusetzen, wobei das Sicherheitsniveau der vorliegend festgelegten Maßnahmen nicht unterschritten werden darf. Der Auftragnehmer wird sämtliche Änderungen dokumentieren und den Auftraggeber über wesentliche Änderungen unverzüglich in Kenntnis setzen.

§ 5 Umgang mit Rechten der betroffenen Personen

- (1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anfragen seitens betroffener Personen in Bezug auf deren Datenschutzrechte.
- (2) Der Auftragnehmer wird Daten, die im Auftrag verarbeitet werden, nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers beauskunften, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich bei Ausübung ihrer Datenschutzrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

§ 6 Einsatz von Unterauftragnehmern

- (1) Der Auftragnehmer ist berechtigt, Unterauftragnehmer als weitere Auftragsverarbeiter im Rahmen der Verarbeitung personenbezogener Daten einzusetzen. Der Auftraggeber gestattet den Einsatz der in **Anhang 3** aufgeführten Unterauftragnehmer.
- (2) Die Auslagerung auf weitere Unterauftragnehmer sowie jeder Wechsel der gemäß Anhang 3 bestehenden Unterauftragnehmer sind zulässig, soweit:
 - a) der Auftragnehmer eine solche Auslagerung bzw. den Wechsel dem Auftraggeber mit einer Frist von vier (4) Wochen vorab schriftlich oder in Textform anzeigt und
 - b) der Auftraggeber nicht innerhalb von zwei (2) Wochen nach Erhalt der Anzeige gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 – 4 DSGVO mit dem Unterauftragnehmer besteht.
- (3) Im Falle eines Einspruchs des Auftraggebers gegen eine solche Auslagerung bzw. gegen den Wechsel eines Unterauftragnehmers hat der Auftragnehmer das Recht zur außerordentlichen Kündigung dieser Vereinbarung und des Hauptvertrags aus wichtigem Grund.
- (4) Der Auftragnehmer wird die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer unter Berücksichtigung des jeweiligen Risikos vor Beginn der Verarbeitung personenbezogener Daten und sodann regelmäßig kontrollieren.

Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung.

- (5) Sofern der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR erbringt, wird der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch geeignete Maßnahmen, insbesondere durch angemessene Datenschutzgarantien, sicherstellen.
- (6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers schriftlich oder in Textform.
- (7) Im Sinne der vorstehenden Regelungen handelt es sich bei Unterauftragsverhältnissen um solche Leistungen, die sich unmittelbar auf die hauptvertragliche Leistungserbringung beziehen. Hierunter fallen grundsätzlich nicht Nebenleistungen wie z. B. Telekommunikationsdienstleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach dieser Vereinbarung stehen.

§ 7 Rechte und Pflichten des Auftraggebers

- (1) Der Auftraggeber ist für die Beurteilung der Zulässigkeit der Auftragsverarbeitung sowie hinsichtlich der Wahrung der Betroffenenrechte allein verantwortlich.
- (2) Der Auftraggeber hat ein umfassendes Weisungsrecht hinsichtlich der Verarbeitung personenbezogener Daten im Auftrag. Hierzu benennen die Parteien die nachfolgend genannten Personen, die jeweils ausschließlich zur Erteilung und zur Annahme von Weisungen befugt sind:

Befugte Personen bei	Auftraggeber	Auftragnehmer
Name, Vorname	[Name, Vorname]	Neudel, Moritz
E-Mail-Adresse	[E-Mail Kanzlei]	moritz@postfachpilot.de
Dienstliche Telefonnr.	[Telefon Kanzlei]	+49 1734378181

- (3) Eine Änderung von befugten Personen und/oder deren Kontaktdaten ist der jeweils anderen Partei unverzüglich schriftlich oder in Textform mitzuteilen.
- (4) Der Auftraggeber ist verpflichtet, alle Aufträge, Teilaufträge oder Weisungen in dokumentierter Form, d. h. mindestens in Textform, zu erteilen. Nur in dringenden Ausnahmen dürfen Weisungen mündlich erteilt werden; solche Weisungen hat der Auftraggeber unverzüglich und in entsprechender Weise dokumentiert zu bestätigen.
- (5) Der Auftraggeber verpflichtet sich, den Auftragnehmer unverzüglich zu informieren, sofern und soweit er Fehler oder Unregelmäßigkeiten im Rahmen der Auftragsverarbeitung feststellt.
- (6) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften zum Datenschutz sowie die vertraglichen Vereinbarungen, insbesondere die vollständige Umsetzung der festgelegten technisch-organisatorischen Maßnahmen und deren Wirksamkeit, beim Auftragnehmer in angemessenem Umfang selbst oder durch einen im Einzelfall zu benennenden Prüfer zu kontrollieren. Kontrollen sind insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme sowie durch Kontrollen vor Ort möglich. Der Auftragnehmer ist verpflichtet, notwendige Auskünfte zu erteilen und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
- (7) Sofern Kontrollen beim Auftragnehmer vor Ort erforderlich sein sollten, werden diese ohne Störung des Geschäftsbetriebs erfolgen. Solche Kontrollen finden maximal ein (1) Mal jährlich und ausschließlich nach angemessener Vorankündigung während der üblichen Geschäftszeiten des Auftragnehmers statt.

§ 8 Datenverarbeitung außerhalb EU/EWR

- (1) Sofern eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation erforderlich sein sollte, wird der Auftragnehmer die Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO sicherstellen.
- (2) Der Auftraggeber gestattet die Datenübermittlung in ein Drittland an die in Anhang 3 genannten Empfänger. Aus dem Anhang ergeben sich die vom Auftraggeber genehmigten Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung.
- (3) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung der Regelungen nach Kapitel V der DSGVO allein verantwortlich.

§ 9 Beendigung der Verarbeitung im Auftrag

- (1) Nach Beendigung der Zusammenarbeit wird der Auftragnehmer auf Verlangen des Auftraggebers die personenbezogenen Daten gemäß der vereinbarten Aufbewahrungsfrist an den Auftraggeber übergeben und anschließend von den Servern löschen. Dieses Verlangen hat der Auftraggeber binnen drei (3) Monaten nach Beendigung der Zusammenarbeit auszuüben. Die Löschung erfolgt dergestalt, dass eine Wiederherstellung mit vertretbarem Aufwand unmöglich ist.
- (2) Der Auftragnehmer wird die Löschung auch gegenüber seinen Unterauftragnehmern sicherstellen, soweit dies vertraglich möglich und rechtlich zulässig ist.
- (3) Der Auftragnehmer ist zum Nachweis der ordnungsgemäßen Löschung verpflichtet und wird diesen dem Auftraggeber entsprechend vorlegen. Der Auftragnehmer ist berechtigt, Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, entsprechend den jeweiligen Aufbewahrungsfristen auch über die Laufzeit dieser Vereinbarung hinaus aufzubewahren.

§ 10 Schlussbestimmungen

- (1) Diese Vereinbarung gilt vorrangig, auch soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, es sei denn, die Parteien haben ausdrücklich etwas anderes vereinbart.
- (2) Diese Vereinbarung ersetzt alle mündlichen oder schriftlich getroffenen Abreden, die zuvor zwischen den Parteien hinsichtlich des Gegenstands der Verarbeitung getroffen wurden.
- (3) Darüber hinaus gehende mündliche oder schriftliche Nebenabreden zu dieser Vereinbarung wurden nicht getroffen.
- (4) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform, soweit nicht eine Individualvereinbarung getroffen wurde. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.
- (5) Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der Vereinbarung sowie der verbleibenden Bestimmungen im Übrigen nicht berührt. Die Parteien werden sich bemühen, eine wirksame und durchführbare Bestimmung zu vereinbaren, die dem verfolgten wirtschaftlichen Zweck der unwirksamen oder undurchführbaren Bestimmung am nächsten kommt. Dies gilt gleichermaßen im Falle einer Regelungslücke.
- (6) Die nachstehend aufgeführten Anhänge zu dieser Vereinbarung sind integraler und wesentlicher Vertragsbestandteil:

Anhang 1: Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB) und des Sozialgeheimnisses (§ 78 SGB X)

Anhang 2: Technisch-organisatorische Maßnahmen („TOMs“) beim Auftragnehmer

Anhang 3: Genehmigte Unterauftragnehmer

Unterschriften der Parteien:

Ort, Datum

Ort, Datum

Formivio UG (haftungsbeschränkt)
Auftragnehmer

[Name der Kanzlei]
Auftraggeber

Anhang 1 – Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB) und des Sozialgeheimnisses (§ 78 SGB X)

Verschwiegenheitsverpflichtung

zur Verpflichtung auf die Schweigepflicht im Sinne des § 203 StGB sowie auf das Sozialgeheimnis nach § 35 SGB I, § 78 SGB X

Zwischen

[Name der Steuerkanzlei / Steuerberatungsgesellschaft]

[Straße und Hausnummer]

[PLZ und Ort]

– nachfolgend „Auftraggeber“ genannt –

und

Formivio UG (haftungsbeschränkt)

vertreten durch den Geschäftsführer Moritz Neudel

Steinwiesenweg 12

86938 Schondorf am Ammersee

– nachfolgend „Auftragnehmer“ genannt –

wird die nachfolgende Vereinbarung zur Verpflichtung des Auftragnehmers auf die Schweigepflicht im Sinne des § 203 StGB sowie auf das Sozialgeheimnis nach § 35 SGB I, § 78 SGB X getroffen.

1. Zweck der Vereinbarung

- (1) Der Auftraggeber ist als sogenannter Berufsgeheimnisträger nach § 203 StGB verpflichtet, Geheimnisse, die ihm im Zusammenhang mit seiner Tätigkeit anvertraut werden, geheim zu halten. Eine unbefugte Offenbarung eines solchen Geheimnisses durch den Auftraggeber ist strafbar.
- (2) Der Auftragnehmer wirkt durch das Erbringen seiner Leistungen an der beruflichen oder dienstlichen Tätigkeit des Auftraggebers im Sinne des § 203 Abs. 3 StGB mit.
- (3) Da der Auftraggeber wegen § 203 Abs. 4 Nr. 1 StGB gesetzlich verpflichtet ist, den Auftragnehmer auf die Geheimhaltung im Sinne des § 203 StGB zu verpflichten, dient diese Vereinbarung der Umsetzung dieser Geheimhaltungsverpflichtung des Auftragnehmers.
- (4) Soweit der Auftraggeber Sozialdaten verarbeitet, die dem Sozialgeheimnis nach § 35 SGB I in Verbindung mit § 78 SGB X unterliegen, gilt diese Verpflichtung entsprechend auch für diese Daten; der Auftragnehmer wird Sozialdaten ausschließlich im Rahmen der zulässigen Zweckbindung verarbeiten.

2. Verschwiegenheitspflicht des Auftragnehmers

- (1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber dazu, alle Informationen, von denen er im Zusammenhang mit der Mitwirkung an der beruflichen oder dienstlichen Tätigkeit des Auftraggebers in dessen Funktion als Berufsgeheimnisträger Kenntnis erlangt, strikt geheim zu halten. Dies gilt für Sozialdaten i. S. d. § 78 SGB X entsprechend.
- (2) Die Verpflichtung beinhaltet insbesondere, dass der Auftragnehmer die betreffenden Informationen keiner anderen natürlichen oder juristischen Person offenlegt, ohne dass der Auftraggeber dies zumindest in Textform erlaubt hat.
- (3) Der Auftragnehmer wird im Zusammenhang mit seiner Tätigkeit in seinem Verantwortungsbereich dafür Sorge tragen, dass er nur insoweit Kenntnis von Informationen erhält, wie es für die Erbringung seiner Leistungen aus dem mit dem Auftraggeber geschlossenen Hauptvertrag erforderlich ist.
- (4) Der Auftragnehmer ist verpflichtet, erhaltene Informationen, die der Schweigepflicht unterliegen, in seinem Verantwortungsbereich durch technische und organisatorische

Maßnahmen, die dem Stand der Technik entsprechen, vor der unbefugten Kenntnisnahme durch Dritte zu schützen. Dies beinhaltet auch, dass Beschäftigte des Auftragnehmers, die nicht an der Leistungserbringung beteiligt sind, keinen Zugriff auf die Informationen erhalten.

3. Unterauftragnehmer

- (1) Sofern der Auftragnehmer bei der Erbringung seiner Leistungen für den Auftraggeber in dessen Funktion als Berufsgeheimnisträger selbst Unterauftragnehmer einsetzen möchte, bedarf dies der vorherigen Zustimmung des Auftraggebers in Textform.
- (2) Im Falle einer Zustimmung des Auftraggebers wird der Auftragnehmer dem Unterauftragnehmer erst dann Informationen offenlegen, wenn der Unterauftragnehmer in gleicher Weise wie der Auftragnehmer von diesem auf die Geheimhaltung verpflichtet wurde.
- (3) Der Auftragnehmer wird dem Auftraggeber die Verpflichtung zur Geheimhaltung des Unterauftragnehmers auf Anfrage nachweisen.

4. Hinweis zur Strafbarkeit

- (1) Der Auftraggeber weist den Auftragnehmer darauf hin, dass eine unbefugte Offenbarung von Informationen, die der Auftragnehmer bei der Erbringung seiner Leistungen für den Auftraggeber in dessen Funktion als Berufsgeheimnisträger erlangt hat, nach § 203 Abs. 4 Satz 1 StGB strafbar ist und mit einer Freiheitsstrafe von bis zu einem Jahr oder mit Geldstrafe geahndet werden kann.
- (2) Der Auftraggeber weist den Auftragnehmer weiter darauf hin, dass eine unbefugte Offenbarung an Unterauftragnehmer, die an der Erbringung der Leistung für den Auftraggeber in dessen Funktion als Berufsgeheimnisträger mitwirken, nach § 203 Abs. 4 Nr. 2 StGB strafbar ist, wenn der Unterauftragnehmer nicht ebenfalls auf die Geheimhaltung im Sinne des § 203 StGB verpflichtet wurde. Dies kann ebenfalls mit einer Freiheitsstrafe von bis zu einem Jahr oder mit Geldstrafe geahndet werden. Eine Strafbarkeit entfällt, wenn der Unterauftragnehmer selbst auch Berufsgeheimnisträger im Sinne des § 203 Abs. 1 und 2 StGB ist.
- (3) Der Auftraggeber weist den Auftragnehmer darauf hin, dass eine Verwertung von Informationen, von denen er im Zusammenhang mit der Mitwirkung an Leistungen des Berufsgeheimnisträgers Kenntnis erhält, ebenfalls nach § 204 StGB strafbar ist und mit einer Freiheitsstrafe von bis zu zwei Jahren oder mit Geldstrafe geahndet werden kann.
- (4) Soweit Sozialdaten betroffen sind, weist der Auftraggeber darauf hin, dass auch die unbefugte Offenbarung oder Verwertung von Sozialdaten, die dem Sozialgeheimnis nach § 35 SGB I, § 78 SGB X unterliegen, unzulässig ist und straf- bzw. bußgeldbewehrt sein kann.

5. Verpflichtung von Beschäftigten

- (1) Der Auftragnehmer verpflichtet sich, seine Beschäftigten, die an der Leistungserbringung für den Auftraggeber mitwirken, in gleicher Weise nach den Vorgaben in Ziffer 2 bis 4 dieser Vereinbarung zu verpflichten. Die Verpflichtung hat zu erfolgen, bevor die Beschäftigten erstmals Kenntnis von Informationen, die der Schweigepflicht unterliegen, erhalten.
- (2) Die Verpflichtung hat zumindest in Textform zu erfolgen und ist dem Auftraggeber auf Anfrage nachzuweisen.

6. Dauer der Verpflichtung

Diese Verschwiegenheitsverpflichtung gilt zeitlich unbegrenzt und besteht auch nach Beendigung der Zusammenarbeit zwischen den Parteien uneingeschränkt fort.

Auftraggeber

Auftragnehmer

Ort, Datum

Ort, Datum

[Name der Kanzlei] (Auftraggeber)

Formivio UG (haftungsbeschränkt) (Auftragnehmer)

Anhang 2 – Technisch-organisatorische Maßnahmen („TOMs“) beim Auftragnehmer

Da der Auftraggeber als Berufsgeheimnisträger besonders schützenswerte, dem Berufs- und ggf. Sozialgeheimnis unterliegende Daten verarbeitet, ist ein entsprechend hohes Schutzniveau vorgesehen. Die nachfolgend aufgeführten technisch-organisatorischen Maßnahmen sind beim Auftragnehmer und/oder seinen Unterauftragnehmern umgesetzt:

1. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Verschlüsselte Datenübertragung ausschließlich über TLS/HTTPS zwischen allen Komponenten, Schnittstellen und Diensten.
- Verschlüsselung gespeicherter Daten (Encryption at Rest) auf den eingesetzten Servern und Diensten.
- Zugriff auf die E-Mail-Postfächer ausschließlich über tokenbasierte, verschlüsselte Schnittstellen (OAuth2 / Microsoft Graph); es werden keine Postfach-Passwörter gespeichert.
- Zugangs- und Schnittstelle Geheimnisse (API-Schlüssel, Token) werden geschützt im Secret-Store des Systems abgelegt und nicht im Klartext gespeichert.
- Datenminimierung: Es werden nur die für die Leistungserbringung erforderlichen Daten verarbeitet.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle: Verarbeitung in einem nach ISO 27001 zertifizierten Rechenzentrum (Hetzner, Nürnberg, EU) mit physischer Zutrittskontrolle, Vereinzelung, Videoüberwachung und Zutrittsprotokollierung durch den Rechenzentrumsbetreiber.
- Zugangskontrolle: Systemzugang ausschließlich für den Auftragnehmer über individuelle Benutzerkonten mit starken Passwörtern und Zwei-Faktor-Authentifizierung; Server-Zugang nur über SSH-Schlüsselauthentifizierung; Absicherung durch Firewall und Reverse Proxy, keine offenen administrativen Dienste im öffentlichen Netz.
- Zugriffskontrolle: rollenbasierte Zugriffsrechte nach dem Need-to-know-Prinzip; Zugriff auf personenbezogene Daten ausschließlich durch den Auftragnehmer; Protokollierung administrativer Zugriffe.
- Trennungskontrolle: logische Trennung der Daten je Kanzlei und Mandant innerhalb der eingesetzten Systeme; Trennung von Test- und Produktivumgebung.

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabe-/Transportkontrolle: Übermittlung personenbezogener Daten ausschließlich verschlüsselt (TLS); auf die vereinbarten Postfächer beschränkter Zugriff (Application Access Policy in Microsoft 365).
- Eingabe- und Nachvollziehbarkeitskontrolle: Protokollierung relevanter Verarbeitungsvorgänge im n8n-System (Nachvollziehbarkeit von Vorgang und Zeitpunkt).
- Human-in-the-Loop: Alle KI-generierten Ergebnisse werden ausschließlich als Entwurf bereitgestellt und erst nach Freigabe durch die Kanzlei versendet; es erfolgt keine automatisierte Entscheidung mit Rechtswirkung. Die finale Kontrolle liegt stets beim Auftraggeber.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Regelmäßige, automatisierte Backups und getestete Wiederherstellbarkeit der Systeme und Daten.
- Hosting in einem nach ISO 27001 zertifizierten Rechenzentrum mit redundanter Strom- und Netzanbindung.
- Fehler- und Verfügbarkeits-Monitoring mit automatisierter Benachrichtigung bei Störungen.
- Schutz vor Schadsoftware und unbefugten Netzwerkzugriffen durch Firewall und zeitnahes Einspielen sicherheitsrelevanter Updates.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Auftragskontrolle: Verarbeitung ausschließlich auf dokumentierte Weisung des Auftraggebers.
- Auswahl der Unterauftragnehmer nach Datenschutzkriterien; Abschluss von AVV/DPA mit allen Unterauftragnehmern.
- Verpflichtung aller mitwirkenden Personen auf Vertraulichkeit, § 203 StGB und – soweit Sozialdaten verarbeitet werden – § 78 SGB X.
- Regelmäßige Überprüfung und Aktualisierung der technisch-organisatorischen Maßnahmen.
- Dokumentierter Prozess zur Erkennung, Meldung und Bearbeitung von Verletzungen des Schutzes personenbezogener Daten (Art. 33, 34 DSGVO) mit unverzüglicher Information des Auftraggebers.

Anhang 3 – Genehmigte Unterauftragnehmer

Der Auftraggeber genehmigt den Einsatz der nachfolgend aufgeführten Unterauftragnehmer des Auftragnehmers:

Name des Unterauftragnehmers	Anschrift / Land	Leistungsinhalt	Geeignete Garantien für eine etwaige Drittlandübermittlung
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland (Rechenzentrum Nürnberg, EU)	Server-Hosting / IT-Infrastruktur (selbstgehostetes n8n)	EU/EWR – keine Drittlandübermittlung; AVV nach Art. 28 DSGVO
Mistral AI SAS	15 rue des Halles, 75001 Paris, Frankreich (EU)	KI-gestützte Verarbeitung (Klassifizierung der Eingänge, Erstellung von Textentwürfen)	EU/EWR – keine Drittlandübermittlung; DPA nach Art. 28 DSGVO
Microsoft Ireland Operations Ltd. (Microsoft Corp.)	One Microsoft Place, Dublin 18, Irland; Verarbeitung in der Azure-Region EU	OCR (Azure AI Document Intelligence) und E-Mail-Zugriff (Microsoft Graph / Outlook), beschränkt auf vereinbarte Postfächer	EU Data Boundary; im Übrigen EU-Standardvertragsklauseln (Microsoft Products and Services DPA) sowie aktive Zertifizierung unter dem EU-US Data Privacy Framework