Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 DS-GVO (Auftragsverarbeitung)

zwischen dem Verantwortlichen

_____

_____

_____

– nachfolgend „**Auftraggeber**“ genannt –

und dem Auftragsverarbeiter

Nagl Papierverarbeitung GmbH

– nachfolgend „**Auftragnehmer**“ genannt –.

Präambel

Der Auftraggeber beauftragt den Auftragnehmer mit Lettershopdienstleistungen.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner, die sich aus der Beauftragung des Auftragnehmers mit Hauptvertrag vom ergeben.

Er findet Anwendung auf alle Tätigkeiten, bei denen der Auftragnehmer personenbezogene Daten des Auftraggebers erhebt, verarbeitet und/oder nutzt.

§ 1

Definitionen

1. „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, Art, 4 Nr. 1 DS-GVO.
2. „Datenverarbeitung“ oder „Verarbeitung“ ist jede mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung, Art. 4 Nr. 2 DS-GVO.
3. „Weisung“ ist die auf eine bestimmte Verarbeitung (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers im Sinne des Art. 29 DS-GVO. Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können vom Auftraggeber danach Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

§ 2

Vertragsgegenstand; Ort der Verarbeitung; Laufzeit und Kündigung

1. Der Auftraggeber beauftragt den Auftragnehmer gemäß Art. 4, Abs. 2, 28 DS-GVO mit der Verarbeitung von personenbezogenen Daten zu den unter § 2 Abs. 2 ausschließlich und abschließend genannten Zwecken und im dort abschließend aufgeführten Umfang.
2. Vertragsgegenstand: Gegenstand dieses Vertrages ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

   Lettershopleistungen
3. Ort der Datenvereinbarung: Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, EU-Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
4. Dauer des Auftrags, Kündigung: Der Vertrag

   ☐ beginnt am

   endet am

   oder

   ☒ wird auf unbestimmte Zeit geschlossen. Der Vertrag ist unter Einhaltung der gesetzlichen Kündigungsfrist kündbar, vom Auftragnehmer jedoch frühestens zum Ende des Hauptvertrages.

   Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflicht en stellt solchen schwerwiegenden Verstoß dar.]

§ 3

Art und Zweck der Verarbeitung; Art der personenbezogenen Daten sowie Kategorien betroffener Personen

1. Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten (Art der Verarbeitung entsprechend der Definition von Art. 4 Nr. 2 DS-GVO)

   ☐ Ist konkret beschrieben in der Leistungsvereinbarung vom

   oder

   ☒ Konkrete Beschreibung des Auftragsgegenstandes im Hinblick auf

   Umfang, Art und Zweck der Aufgaben des Auftragnehmers:

   Der Auftragnehmer übernimmt personenbezogene Daten von uns bzw. erhält direkt Daten von unseren Kunden und verarbeitet sie weiter (Reihenfolge ändern, Dublettenabgleich, etc.) zum anschließenden Druck. Er druckt die verarbeiteten Daten auf gestellte Druckbogen, Kuverts, im Anschluss weiterverarbeitet werden (geschnitten, gefalzt, kuvertiert, postaufgeliefert, etc.). Datenkorrekturen oder -änderungen erfolgen ausschliesslich nach expliziter Anweisung des Kunden.

2. Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

   Personenstammdaten

   Kommunikationsdaten (z.B. Telefon, E-Mail)

   Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw.

   Vertragsinteresse)

   Kundenhistorie

   Vertragsabrechnungs- und Zahlungsdaten

   Planungs- und Steuerungsdaten

   Daten zu Bank- Kreditkartenkonten, Fahrgestellnummer

3. Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO)

   Kunden,Interessenten, Abonnenten, Beschäftigte, Lieferanten, Handelsvertreter

Ansprechpartner

4. Der Auftraggeber kann auch nach der Laufzeit des Vertrages und nach Beendigung des Vertrages die Herausgabe oder Löschung der Auftraggeber-Daten verlangen, soweit diese nicht schon aufgrund Zweckwegfall oder sonstiger gesetzlicher oder vertraglicher Fristen gelöscht sind.

   Die Inhalte dieses Vertrages gelten entsprechend, wenn und soweit vom Auftragnehmer die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 4

Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.
2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format (via E-Mail ist ausreichend) festzulegen.
3. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format (via E-Mail ist ausreichend). Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
4. Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
5. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

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

§ 5

Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

1. Weisungsberechtigte Personen des Auftraggebers sind:

2. Weisungsempfänger beim Auftragnehmer sind:

   Ulrike Schwertz, Leitung Lettershop, 089 69798726

3. Für Weisung zu nutzende Kommunikationskanäle:

   Nagl Papierverarbeitung GmbH, Martin Festl Ring 8, 85609 Aschheim, info@nagl-papierverarbeitung.de, 089 697987-0

4. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch (per E-Mail ist ausreichend) die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§ 6

Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

2. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Ko-

pien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
4. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
5. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

   Weisungsberechtigter des Auftraggebers gemäß § 5.
6. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.
7. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.
8. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
9. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

10. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt:

    Der Auftragnehmer hat dem Auftraggeber auf Anforderung geeigneten Nachweis über die Einhaltungen der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigte Verhaltensregeln i.S.v. Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren i.S.v. Art. 42 DSGVO abbilden, erbracht werden.

11. Der Auftragnehmer gewährt dem Auftragnehmer bzw. von diesen beauftragten Dritten – auf Anforderung und nach rechtzeitiger vorheriger Ankündigung – Zugang in die zur Datenverarbeitung genutzten Räumlichkeiten bei sich oder bei Unterauftragsnehmern. Er stellt in ausreichendem Umfang fach- und sachkundiges Personal in zumutbarem Umfang ab. Diese Leistungen erfolgen kostenfrei. Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

12. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er sicher weiter zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

13. Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr/Frau

    Dominik , Fünkner, Datenschutzexperte.de, Tel+49 89 2500392 22

    bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

14. Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

§ 7

Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. § 4 dieses Vertrages durchführen.

§ 8

Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

1. Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der nach dieser Vereinbarung für eine auftraggeberseitige Weisung zulässig erklärten Kommunikationswege erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
2. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
3. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des

Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

4. Der Vertrag mit dem Subunternehmer muss schriftlich oder in elektronischem Format gemäß Art. 28 Abs. 4 und Abs. 9 DS-GVO abgeschlossen werden.
5. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.
6. Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) entsprechend den Regelungen, die zwischen Auftragnehmer und Auftraggeber nach dieser Vereinbarung getroffen wurden, zu überprüfen.
7. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.
8. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden oder an die er von Gesetzes wegen unter der DS-GVO gebunden ist.
9. Zurzeit sind für den Auftragnehmer die in **Anlage 2** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.
10. Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

§ 9

Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme

und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

☒ vorhanden siehe Anlage 1 der Firma Nagl Papierverarbeitung GmbH

2. Das im **Anlage 1** beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.
3. Die datenschutzkonforme Verarbeitung wird durch ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen sichergestellt. Der Auftragnehmer stellt dem Auftraggeber entsprechende Dokumentationen auf Anforderung zur Verfügung.
4. Der Auftragnehmer hat regelmäßig eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO).
5. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.
6. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.
7. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

§ 10

Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

1. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und er-

stellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

§ 11

Haftung

Es gilt Art. 82 DS-GVO. Es wird klargestellt, was folgt: Der Auftragsverarbeiter haftet für Verstöße von ihm eingeschalteter Subunternehmer wie für eigenes Verschulden, und zwar unabhängig davon, ob der Auftraggeber der Einschaltung zugestimmt hat.

§ 12

Sonstiges; **Schlussbestimmungen**

1. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren
2. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Sollten Auftraggeber-Daten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Auftraggeber-Daten beim Auftraggeber liegt.
3. Nebenabreden zu diesem Vertrag wurden nicht getroffen. Änderungen und Ergänzungen des Vertrages, soweit es sich nicht um Weisungen handelt, bedürfen zu ihrer Rechtswirksamkeit der Schriftform oder sind in einem dokumentierten elektronischen Format vorzunehmen. Dies gilt auch für die Aufhebung dieses Vertrages oder die Änderung des Formerfordernisses.
4. Sollte eine Bestimmung dieses Vertrages ganz oder teilweise unwirksam sein oder ihre Rechtswirksamkeit später verlieren, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen Bestimmung soll – soweit rechtlich zulässig – eine andere angemessene Regelung gelten, die dem am nächsten kommt, was die Vertragsparteien gewollt haben

oder gewollt haben würden, wenn sie die Unwirksamkeit der Regelung bedacht hätten. Entsprechendes gilt, sofern und soweit der Vertrag eine Lücke aufweist; diese soll durch eine Regelung geschlossen werden, die dem entspricht, was die Vertragsparteien gewollt haben oder gewollt haben würden, wenn sie die Lückenhaftigkeit des Vertrages insoweit bedacht hätten.

5. Der Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist München.
6. Folgende Anlage zu diesem Vertrag ist wesentlicher Bestandteil desselben:

Anlage 1 - Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Anlage 2 – Subunternehmer

Ort , Datum	Ort , Datum
Auftraggeber - Firma	Auftragnehmer - Firma
Auftraggeber - Name	Auftragnehmer - Name

Anlage 1:

Diese Anlage zu den Technisch-organisatorischen Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO ist vom Verantwortlichen (Art. 30 Abs.1 lit g) wie auch vom Auftragsverarbeiter (Art. 30 Abs. 2 lit d) zwingend entsprechend seiner innerbetrieblichen Organisation auszufüllen. Wo zutreffend, können Referenzen auf die zur Verfügung gestellten Dokumente/Zertifikate (Ziffer 12 dieser Anlage) angegeben werden. Die innerbetriebliche Organisation ist vom Verantwortlichen/Auftragsverarbeiter so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dies beinhaltet insbesondere:

1. Zutrittskontrolle zu Räumlichkeiten und Einrichtungen, in denen Daten verarbeitet werden

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen, nach dem jeweiligen Stand der Technik, zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

Schlüsselregelung (Schlüsselausgabe etc.)

Manuelles Schließsystem

Videoüberwachung der Zugänge

Sorgfältige Auswahl von Reinigungspersonal

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme (IT-Systeme) ist zu verhindern.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:
Zuordnung von Benutzerrechten
Passwortvergabe
Authentifikation mit Benutzername / Passwort
Gehäuseverriegelungen (Server)
Sperren von externen Schnittstellen (USB etc.)
Schlüsselregelung (Schlüsselausgabe etc.)
Einsatz von Anti-Viren-Software
Einsatz einer Hardware-Firewall
Erstellen von Benutzerprofilen
Einsatz von VPN-Technologie
Sorgfältige Auswahl von Reinigungspersonal
Verschlüsselung von Datenträgern in Laptops / Notebooks
Einsatz einer Software-Firewall

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen (IT-Systemen) außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

Erstellen eines Berechtigungskonzepts
Anzahl der Administratoren auf das „Notwendigste“ reduziert
Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
Verwaltung der Rechte durch Systemadministrator
Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
Protokollierung der Vernichtung

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln (Elektronische Übertragung, Datentransport, Übermittlungskontrolle, usw.), um einen Verlust, eine Veränderung oder eine unbefugte Veröffentlichung zu verhindern.

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

E-Mail-Verschlüsselung

5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten derart, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen; Art. 32.I.a) DSGVO; Art. 25.I DSGVO)

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

Im Dialogpostmangager werden die Daten nach Abschluss des Mailing pseudonysiert

(z.B. Maßnahmen, bei denen Pseudonymisierung angewandt wird – sofern dies zur notwendig ist um ein angemessenes Schutzniveau zu gewährleiten)

6. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

Protokollierung der Eingabe, Änderung und Löschung von Daten

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche

Daten eingegeben, geändert und gelöscht werden können.

7. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten. Eine Datenverarbeitung durch Dritte (vergleiche Artikel 28 DSGVO) ist gemäß den Anweisungen des Auftraggebers/Datenexporteurs erlaubt. Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber/Datenexporteur und Auftragnehmer/Datenimporteur:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)
Auftragnehmer hat Datenschutzbeauftragten bestellt
Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

8. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

Unterbrechungsfreie Stromversorgung (USV)
Testen von Datenwiederherstellung
Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
Schutzsteckdosenleisten in Serverräumen
Erstellen eines Notfallplans
Serverräume nicht unter sanitären Anlagen

9. Getrennte Verarbeitung von Daten

Die getrennte Verarbeitung von Daten, die für unterschiedliche Zwecke gesammelt wurden.

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
Erstellung eines Berechtigungskonzepts
Logische Mandantentrennung (softwareseitig)

10. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

Interne Mandantenfähigkeit
Physikalsiche oder logische Trennung

11. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32.I. d) DSGVO; Art. 25.I DSGVO)

☒ Datenschutz-Management;

☒ Incident-Response-Management;

☒ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

☒ Auftragskontrolle i.S.v. Art. 28 DSGVO

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen - Detaillierte Beschreibung:

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Prüfprotokoll, Datenkontrolle durch weiteren Mitarbeiter

Eindeutige Vertragsgestaltung, sorgfältige Auswahl des Auftragnehmers, Kontrolle der Vertragsausführung

12. Ergänzende oder erklärende Dokumente und/oder Zertifikate

Bitte ankreuzen und zur Verfügung stellen.

☐ ISO27001 Zertifikat
☐ Binding Corporate Rules (BCR)
☒ Sicherheitskonzept
☐ DSGVO (GDPR) Zertifikat (nach Art. 42 DSGVO/GDPR)
☐ TISAX Zertifikat

einfach. sicher. schnell.

Anlage 2 - Subunternehmer

Die vertraglich vereinbarten Leistungen/Teilleistungen werden unter Einschaltung von Subunternehmen durchgeführt, die in diese Verarbeitung mit einbezogen sind.

☐ Es werden keine Subunternehmer beschäftigt

oder

☒ Es werden Subunternehmer beschäftigt

- ☒ nur aus dem Inland
- ☐ auch aus EU/EWR-Raum
- ☐ auch aus Drittstaaten außerhalb dem EWR / der EU

Nachstehend werden alle Subunternehmer aufgeführt, **die unmittelbar mit der Leistungserstellung für den Auftraggeber beteiligt sind** und möglicherweise Zugriff auf die Daten des Auftraggebers haben oder haben könnten. Dazu zählen auch externe IT-Dienstleister mit entsprechenden Zugriffsrechten. Nicht dazu gehören i. d. R. Telekommunikationsleistungen, Post-/Transportdienstleistungen.

Subunternehmer Firma, Ort und Ansprechpartner	**Leistungsbesbreibung** (Tätigkeit des Subunternehmers)
1. Fourkioti Anastasia, 85609 Aschheim, Frau Anastasia Fourkioti	ausschließlich Datenverarbeitung in bereits von Fa. Nagl ausgedruckter und verarbeiteter Papierform
2. Bernhard Boxhorn Boxhorn EDV., 81379 München, Herr Bernhard Boxhorn	IT Dienstleister, Systemadministrator
3.	
4.	