Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO

Hiermit beauftrage ich die

A&O Fischer GmbH & Co. KG
Maybachstraße 9
21423 Winsen/Luhe

zur Datenverarbeitung gemäß des vorliegenden Vertrages.

1 **Einführung**

1.1 Die Rechtslage ändert sich mit Anwendbarkeit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (EU – Datenschutzgrund-verordnung – (kurz: DS-GVO) ab 25.05.2018. Auch das Bundesdatenschutzgesetz ist mit dem Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30.06.2017 (Datenschutz-Anpassungs- und- Umsetzungsgesetz EU – DSAnpUG –EU) neu gefasst.

2 **Gegenstand und Dauer der Vereinbarung**

2.1 Der Gegenstand des Auftrages ergibt sich aus **Anlage 1**.

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

2.3 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, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2.4 Diese Vereinbarung wird zum 25.5.2018 wirksam und ersetzt bisherige zur Auftragsverarbeitung getroffenen Vereinbarungen zum Datenschutz und zur Datensicherheit.

3 **Dauer des Auftrags**

3.1 Die Dauer des Auftrages ergibt sich aus der **Anlage 1**.

3.2 Der Auftraggeber kann den Vertrag ohne Einhaltung einer Frist ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO grob fahrlässig oder vorsätzlich verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen, mithin weder vorsätzlichen noch grob fahrlässigen Verstößen setzt der Auftraggeber eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

4 **Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen**

4.1 Die Art, der Zweck, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen ergibt sich aus **Anlage 1** bzw. aus der Leistungsbeschreibung des Hauptvertrages.

5 **Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers**

5.1 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 aus-schließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

5.2 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

5.3 Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

5.4 Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt 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.

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

5.6 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.

5.7 Die Weisungsberechtigten des Auftraggebers sowie die Weisungsempfänger des Auftragnehmers ergeben sich aus der **Anlage 1.**

5.8 Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

5.9 Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

6 Pflichten des Auftragnehmers

6.1 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).

6.2 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

6.3 Der Auftragnehmer verpflichtet sich, im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung gemäß den vereinbarten Maßnahmen vorzunehmen.

6.4 Er gewährleistet, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert. Das Ergebnis der Kontrollen ist zu dokumentieren.

6.5 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 gegen Vergütung 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 die weisungsberechtigte Person des Auftraggebers weiterzuleiten.

6.6 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.

6.7 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.

6.8 Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung zu üblichen Bürozeiten und mit angemessener Vorlaufzeit - 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). Der Auftragnehmer hat das Recht seinen Datenschutzbeauftragten hinzuziehen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrolle, sofern davon die Betriebsabläufe des Auftragnehmers gestört werden, nur im erforderlichen Umfang durchgeführt wird.

6.9 Der Auftragnehmer ist verpflichtet, soweit erforderlich, bei diesen Kontrollen gegen Vergütung unterstützend mitwirkt.

6.10 Für die Verarbeitung von Daten in Privatwohnungen oder mobil hat der Aufragnehmer mit seinen Mitarbeitern eine Regelung getroffen, die den datenschutzrechtlichen Anforderungen entspricht. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall getroffen.

6.11 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich auch gemäß **Anlage 1** für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen.

6.12 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

6.13 Der Auftragnehmer verpflichtet sich, 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 DSGVO).

6.14 Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb. Die/Der Beauftragte(r) für den Datenschutz Herr/Frau des Auftragnehmers ergibt sich aus **Anlage 1**. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

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

7 Vergütung

Für Verpflichtungen aus diesem Vertrag gilt: Kosten für etwaige Unterstützungsleistungen benennt der Auftragnehmer vorab und sind gemäß Vereinbarung vom Auftraggeber zu zahlen.

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

8.1 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.

8.2 Der Auftragnehmer verpflichtet sich, 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. Ziff. 4 dieses Vertrages durchführen.

8.3 Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48

Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

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

9.1 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 o.g. Kommunikationswege (Ziff. 4) erfolgen muss.

9.2 Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt.

9.3 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 Auftrag-geber auf Anfrage zur Verfügung zu stellen.

9.4 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).

9.5 Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten.

9.6 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.

9.7 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.

9.8 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

9.9 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.

9.10 Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

9.11 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.

9.12 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.

9.13 Der Auftragsverarbeiter informiert den Verantwortlichen immer 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). Die Bestellung des Unterauftragnehmers, gegen den Einspruch erhoben wurde, ist nicht möglich.

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

10.1 Es wird für die konkrete Auftragsverarbeitung, ein dem Risiko für die Rechte und Freiheiten, der von der Verarbeitung betroffenen natürlichen Personen, angemessenes Schutzniveau gewährleistet.

10.2 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.

10.3 Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.

10.4 Das in **Anlage 2** 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 Verarbeitungs-prozesse beim Auftragnehmer dar.

10.5 Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, 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). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber auf Anfrage mitzuteilen.

10.6 Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

10.7 Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

10.8 Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

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

11.1 Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

11.2 Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

12 Haftung

12.1 Auf Art. 82 DS-GVO wird verwiesen. Der Auftragnehmer haftet nur dann im Innenverhältnis, wenn der Auftraggeber nachweist, dass der Auftragnehmer für den erlittenen Schaden verantwortlich ist.

12.2 Im Übrigen richtet sich die Haftung nach den getroffenen Vereinbarungen aus dem Hauptvertrag.

13 Sonstiges

13.1 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.

13.2 Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

13.3 Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftrag-nehmer den Auftraggeber unverzüglich zu verständigen.

13.4 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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

Anlage 1

1. Gegenstand und Zweck der Verarbeitung
Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Gegenstand des Auftrags zur Datenverarbeitung ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Die Daten des Kunden werden nach elektronischer Einlieferung durch den Kunden auf Verarbeitbarkeit überprüft. Geprüft werden die möglichen Standardformate (PDF, MS-Word). Darauf aufbauend werden die Druckdaten für die Weitergabe an die Drucker aufbereitet.
Im Rahmen dieses Auftrags können Fehler bei der Verarbeitung auftreten. Bei einem Fehler wird dem Auftragsverarbeiter erlaubt, Zugriff auf die personengebundenen Daten des Kunden zu nehmen. Der Zugriff ist ausschließlich für den Zweck der Fehleranalyse vorgesehen.

2. Art(en) der personenbezogenen Daten
Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

☒ Personenstammdaten
☒ Kommunikationsdaten (z.B. Telefon, Fax, E-Mail)
☒ Vertragsstammdaten (Vertragsbeziehungen, Produkt- bzw. Vertragsinteressen)
☒ Kundenhistorie
☒ Vertragsabrechnungs- und Zahlungsdaten
☒ Sendungsdaten

3. Kategorien betroffener Person
Kreis der von der Datenverarbeitung betroffenen Personen:

☒ Kunden des Auftraggebers, die Briefsendungen erhalten
☒ Beschäftigte des Auftraggebers, die Briefsendungen erhalten
☒ Lieferanten des Auftraggebers, die Briefsendungen erhalten
☒ Ansprechpartner des Auftraggebers
☒ Mitarbeiter und Ansprechpartner von LetterXpress

4. Weisungen des Auftraggebers

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

5. Weisungsempfangsberechtigte Personen des Auftragnehmers:

Angaben zum Auftragsverarbeiter Name und Kontaktdaten, natürliche Person/juristische Person/Behörde/Einrichtung etc.		
Name:	A&O Fischer GmbH & Co. KG	
Straße:	Maybachstraße 9	
PLZ/Ort:	21423 Winsen/Luhe	
Telefon:	+49 4171 6559 0	
E-Mail-Adresse:	info@aof.de	
Internet-Adresse:	www.aof.de	
Angaben zum Vertreter des Auftragsverarbeiters		
Name:	Oliver Fischer	André Fischer
Straße:	Maybachstraße 9	Maybachstraße 9
PLZ/Ort:	21423 Winsen/Luhe	21423 Winsen/Luhe
Telefon:	+49 4171 6559 10	+49 4171 6559 5
E-Mail-Adresse:	o.fischer@aof.de	a.fischer@aof.de
Internet-Adresse	www.aof.de	www.aof.de
Angaben zur Person des Datenschutzbeauftragten (*extern mit Anschrift) *sofern gem. Artikel 37 DS-GVO benannt		
Name:	RAin Carola Sieling c/o Kanzlei Sieling	
Straße:	Gurlittstraße 24	
PLZ/Ort:	20099 Hamburg	
Telefon:		
E-Mail-Adresse:	carola.sieling@kanzlei-sieling.de	
Internet-Adresse:	www.kanzlei-sieling.de	

6. Der Auftragnehmer verpflichtet sich, auch für diesen Auftrag relevante Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen. Der Auftragnehmer ist auf diese besonderen Regeln vom Auftraggeber hinzuweisen (wie z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB).

7. Die Laufzeit dieses Vertrages entspricht der Laufzeit der Leistungsvereinbarung und erlischt automatisch mit der Kündigung des LetterXpress Online Kontos.

8. Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).
Dabei handelt es sich um nachfolgende(s) Unternehmen:

Unterauftragnehmer, Adresse	**Leistung**
Icom Software Research oHG Martin-Schmeißer-Weg 11 44227 Dortmund	IT Service und Support Dienstleistungen
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen	Datensicherung/Backup
Deutsche Post AG Charles-de-Gaulle-Straße 20 53113 Bonn	Konsolidierungs-Dienstleister
Zendesk Inc. 989 Market Street #300 San Fransisco, CA 94102	Ticketsystem Support
Rapidmail GmbH Augustinerplatz 2 79098 Freiburg i.Br.	Kundenmitteilungen, Newsletter
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy L-1855, Luxembourg	Server Infrastruktur
PAYONE GmbH Niederlassung Kiel Fraunhoferstraße 2-4 24118 Kiel	Zahlungsverkehr
Reisswolf Akten und Datenvernichtung GmbH & Co. KG Wendenstraße 403 20537 Hamburg	Datenvernichtung

Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle:
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.

Zweck:
Diese Maßnahmen sollen gewährleisten, dass Unbefugten der „körperliche" Zutritt zu Datenverarbeitungs-anlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird.

Im Unternehmen getroffene Maßnahmen:
- ☐ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- ☒ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, Code-Schloss etc.)
- ☒ Zaunanlagen
- ☒ Sicherheitstüren/-fenster
- ☐ Gitter vor Fenstern/Türen
- ☐ Werkschutz, Pförtner
- ☒ Alarmanlage
- ☒ Videoüberwachung
- ☒ Spezielle Schutzvorkehrungen des Serverraums
- ☒ Mitarbeiter- und Berechtigungsausweise
- ☒ Sperrbereiche
- ☐ Sonstiges

Zugangskontrolle
Kein unbefugter Systemzugang.

Zweck:
Diese Maßnahmen sollen gewährleisten, dass nur befugten Personen die Datenverarbeitungssysteme zugänglich sind und ausschließlich von Ihnen benutzt werden können.

Im Unternehmen getroffene Maßnahmen:
- ☒ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- ☒ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- ☐ BIOS-Passwörter
- ☒ Zusätzlicher System-Log-In für bestimmte Anwendungen
- ☒ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- ☒ Elektronische Dokumentation sämtlicher Passwörter und Verschlüsselung dieser Dokumentation zum Schutz vor unbefugten Zugriff
- ☐ Personalisierte Chipkarten, etc.
- ☐ Sonstiges

Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Zweck:
Diese Maßnahmen sollen gewährleisten, dass nur die zur Nutzung des Datenverarbeitungssystems Berechtigten den Zugriff auf diese Systeme haben und der Zugriff sich ausschließlich auf diese personenbezogenen Daten beschränkt, die dieser Zugriffsberechtigung unterliegen, so dass Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Im Unternehmen getroffene Maßnahmen:
☒ Verwaltung von Berechtigungen
☒ Differenzierte Berechtigungen
☒ Profile
☒ Rollen
☒ Dokumentation von Berechtigungen
☒ Genehmigungsroutine
☒ Auswertungen/Protokollierungen
☒ Prüfung/Auditierung (etwa im Rahmen von ISO-Zertifizierung, SOX-Compliance)
☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, True Crypt, Safe Guard Easy, WinZip, PGP)
☒ Vier-Augen-Prinzip
☒ Segregation of Duties
☒ Aufgabenbezogene Berechtigungsprofile
☒ Passwort-Identifikation, etc.
☐ Sonstiges

Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit, Sandboxing;

Zweck:
Zweckbezogene Verarbeitung personenbezogener Daten soll technisch sichergestellt werden, d.h. zu unterschiedlichen Zwecken erhobene Daten sollen auch entsprechend getrennt verarbeitet werden.

Im Unternehmen getroffene Maßnahmen:
☒ Getrennte Systeme
☒ Getrennte Datenbanken
☒ Zugriffsberechtigungen
☒ Trennung durch Zugriffsregelungen
☐ Sonstiges

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Zweck:
Diese Maßnahmen sollen gewährleisten, dass Datenträger während ihres Transports oder elektronischer Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, bzw. soll durch die Maßnahmen überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personen-bezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Insofern werden die Transport- und Datenträgerkontrollen durch die Weitergabekontrolle zusammengefasst.

Im Unternehmen getroffene Maßnahmen:
☒ Verschlüsselung von Email
☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, True Crypt, Safe Guard Easy, WinZip, PGP)
☒ Getunnelte Datenfernverbindungen (VPN = Virtual Private Network)
☒ Protokollierung
☒ Transportsicherung von Datenträgern und Transportbehältern
☒ Gesichertes WLAN
☒ SSL-Verschlüsselung bei Web-access
☒ Regelungen zur Datenträgervernichtung, etc.
☐ Sonstiges

Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung, Dokumentenmanagement;

Zweck:
Durch diese Maßnahmen soll die Nachprüfbarkeit eines Verarbeitungsvorgangs (Eingabe, Änderung, Entfernung) personenbezogener Daten gewährleistet werden, d.h. Urheber, Inhalt und Zeitpunkt der Datenspeicherung sollen ermittelt werden können.

Im Unternehmen getroffene Maßnahmen:
☒ Zugriffsrechte
☒ Systemseitige Protokollierungen
☒ Sicherheits-/Protokollierungssoftware
☒ Funktionelle Verantwortlichkeiten
☒ Mehraugenprinzip
☐ Sonstiges

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

Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

Zweck:
Es muss sichergestellt sein, dass die personenbezogenen Daten nicht zufällig zerstört werden und vor Verlust geschützt sind.
Es muss gewährleistet sein, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Im Unternehmen getroffene Maßnahmen:
☒ Back-Up Verfahren von Festplatten und Servern
☒ Unterbrechungsfreie Stromversorgung (USV)
☒ Aufbewahrungsmodalitäten von Back-Ups (Safe, getrennter Brandabschnitt, etc.)
☒ Virenschutz /Firewall
☒ Klimaanlage
☒ Brand- und Löschwasserschutz
☒ Alarmanlage
☒ Geeignete Archivierungsräumlichkeiten
☒ Notfallplan
☒ Notfallübungen
☐ Katastrophenpläne
☒ Ausfallpläne und Wiederherstellungspläne, etc.
☐ Sonstiges

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Der Auftragsverarbeiter ist zertifiziert nach DIN ISO 27001;
Zertifikats-ID: DSC.471.07.2017, gültig bis 30.06.2020

Dieses beinhaltet ein nachgewiesenes:

a) Datenschutz-Management;
b) Incident-Response-Management;
c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Zweck:
Der Auftragnehmer hat zu gewährleisten, dass die im Auftrag zu bearbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Mittelbar damit verbunden ist die Pflicht des Auftraggebers, Weisungen an Auftragnehmer zu erteilen.

Im Unternehmen getroffene Maßnahmen:

☒ Schriftlicher Vertrag zur Auftragsverarbeitung gem. DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
☒ Schulungen aller zugriffsberechtigten Mitarbeiter
☒ Regelmäßig stattfindende Nachschulungen
☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis gem. BDSG
☒ Verpflichtung der Mitarbeiter auf das Sozialgeheimnis gem. SGB
☒ Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis gem. § 88 TKG
☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
☒ Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag
☒ Service Level Agreements (SLAs) für den Einsatz von Kontrollen
☐ Sonstiges