Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO

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: DSGVO) 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 DSGVO 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. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2.4 Diese Vereinbarung wird zum 01.07.2022 wirksam und ersetzt bisherige zur Auftragsverarbeitung getroffene Vereinbarungen zum Datenschutz und zur Datensicherheit.

3 **Dauer des Auftrags**

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

3.2 Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte ordentliche Kündigung dieses Vertrags ist ausgeschlossen. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

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 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO 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. 6 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 Der Inhaber des Kundenkontos bei LetterXpress ist weisungsberechtigte Person des Auftraggebers.

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

5.9 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Verlangt der Auftraggeber in solchen Fällen Unterstützung aufgrund von Umständen, die der Auftragnehmer nicht zu vertreten hat, so kann der Auftragnehmer den dadurch ausgelösten Aufwand in Rechnung stellen.

5.10 Der Auftragnehmer wird unverzüglich durch den Auftraggeber informiert über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftraggeber ermittelt.

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 DSGVO).

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

6.3 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.

6.4 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO 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 DSGVO).

6.5 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 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

6.6 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.

6.7 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.

6.8 Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - nach Terminvereinbarung, im Rahmen der üblichen Geschäftszeiten ohne Störung des Betriebsablaufs- und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers - 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 DSGVO).

6.9 Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.

6.10 Der Auftraggeber stimmt den Termin einvernehmlich mit dem Auftragnehmer ab und informiert diesen rechtzeitig (in der Regel mindestens einen Monat vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände.

6.11 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber gegenüber dem Auftragnehmer verpflichtet ist. Zudem muss sich der Dritte auf Verschwiegenheit und Geheimhaltung gegenüber dem Auftragnehmer verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Verpflichtet sich der Dritte nicht zur Verschwiegenheit und Geheimhaltung gegenüber dem Auftragnehmer, so kann der Auftragnehmer die Überprüfung durch den Dritten ablehnen.

6.12 Beabsichtigt der Auftraggeber die Kontrolle durch einen Dritten durchführen zu lassen, so teilt er dies dem Auftragnehmer unter Berücksichtigung der vereinbarten Frist (6.10) mit und identifiziert

den Dritten in hinreichendem Maße. Der Auftragnehmer hat das Recht den Dritten abzulehnen, sofern dessen Einsatz negative Auswirkungen auf den Geschäftsbetrieb haben könnte, die über den Zeitraum der bloßen Vor-Ort-Kontrolle hinausgeht. Dies ist u.a. dann der Fall, wenn der Dritte ein Konkurrent des Auftragnehmers ist oder Konkurrenten des Auftragnehmers betreut und nicht gesetzlich zur Geheimhaltung verpflichtet ist, er bereits Opfer von Whistleblowing oder dem Verrat von Geschäftsgeheimnissen geworden ist, oder selbst Whistleblowing betrieben oder Geschäftsgeheimnisse verraten hat oder, wenn der Dritte durch lokale Gesetze zur Weitergabe der bei der Kontrolle erlangten Informationen verpflichtet wäre oder zu befürchten ist, dass er selbst ohne Rechtsgrundlage zur Weitergabe der Daten aufgrund anderer Umstände dazu gezwungen werden könnte. Der Auftragnehmer kann Ersatz der Kosten für den durch eine Vor-Ort-Kontrolle verursachten Aufwand verlangen.

6.13 Der Nachweis von Maßnahmen zur Erfüllung der Pflichten aus Art. 28 DSGVO kann auch erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO,
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art 42 DSGVO,
- aktuelle Testate Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT- Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder
- eine geeignete Zertifizierung durch IT- Sicherheits- oder Datenschutzaudit z.B. nach ISO 27001 – („Prüfungsbericht“).

6.14 Der Auftragnehmer ist verpflichtet, soweit erforderlich, bei diesen Kontrollen unterstützend mitzuwirken.

6.15 Das Ergebnis einer (etwaigen vorvertraglichen) Kontrolle ist dem Auftragnehmer auf Anfrage in Textform mitzuteilen.

6.16 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.

6.17 Der Auftragnehmer gewährleistet, 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).

6.18 Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb. Die Kontaktdaten der bestellten Datenschutzbeauftragten ergeben sich aus der **Anlage 1**.

6.19 Die vom Auftraggeber an den Auftragnehmer mit Hilfe von LXP TREIBER, LXP GO, BRIEF SCHREIBEN, LXP API oder LXP SFTP übermittelten Daten (Adressdaten der Briefempfänger, textlicher und sonstiger, z.B. bildlicher, Inhalt der Schreiben) werden vom Auftragnehmer zum Zweck der Auftragsverarbeitung und Auftragsverfolgung für 60 Tage gespeichert und anschließend vollständig gelöscht.

7 **Vergütung**

7.1 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

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 DSGVO.

8.2 Der Auftragnehmer gewährleistet, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß dieses Vertrages durchführen.

9 **Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)**

9.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

9.2 Die vertraglich vereinbarten Leistungen bzw. die beschriebenen Teilleistungen werden unter Hinzunahme der in der Anlage 1 genannten Unterauftragsverarbeiter durchgeführt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftraggeber erteilt dem Auftragnehmer hiermit eine allgemeine, schriftliche Genehmigung, andere Auftragsverarbeiter im Rahmen dieses Auftrags in Anspruch nehmen zu können.

9.3 Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung genehmigter Auftragsverarbeiter oder die Verlagerung der Dienstleistung oder Teile jener in ein Drittland, wodurch der Auftraggeber die Möglichkeit erhält, innerhalb von zwei Wochen ab Erhalt dieser Information schriftlich unter Darlegung der Gründe gegen derartige Änderungen Einspruch zu erheben.

9.4 Der Auftragnehmer verpflichtet sich, die besonderen Vorgaben des Art. 44 ff. DSGVO einzuhalten. Der Auftraggeber verpflichtet sich, die notwendigen EU-Standardvertragsklauseln mit den Unterauftragsverarbeitern abzuschließen. Der Auftraggeber kann im Einvernehmen mit dem Auftragnehmer diesen beauftragen, die Standardvertragsklauseln stellvertretend für diesen abzuschließen. Schließt der Verantwortliche selbst die Standarddatenschutzklauseln mit den Unterauftragsverarbeitern ab, so stellt er eine unterzeichnete Kopie dem Auftragnehmer zu Nachweiszwecken zur Verfügung.

9.5 Bei einem Einspruch hat der Auftragnehmer die Wahl, einen anderen Unterauftragnehmer auszuwählen, die Verarbeitung selbst durchzuführen, oder den Hauptvertrag inklusive dieses Vertrages mit zweiwöchiger Frist zum Ende eines Monats zu kündigen.

9.6 Wählt der Auftragnehmer einen neuen Unterauftragnehmer aufgrund des Einspruchs, so teilt er diesen dem Auftraggeber unverzüglich mit. Eventuelle Mehrkosten durch den Einsatz eines anderen Unterauftragsverarbeiters trägt der Auftraggeber. Das Einspruchsrecht des Auftraggebers gilt auch für erneut vorgeschlagene Unterauftragsverarbeiter.

9.7 Der Auftragnehmer hat im Falle einer Beauftragung von anderen Auftragsverarbeitern, im Rahmen der hier vereinbarten Auftragsverarbeitung vertraglich sicherzustellen, dass die vereinbarten Datenschutzpflichten zwischen Auftraggeber und Auftragnehmer gem. Art. 28 Abs. 4 DSGVO auch entsprechend gegenüber den anderen Unterauftragsverarbeitern gelten.

10 **Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)**

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 DSGVO, 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 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 Verarbeitungsprozesse beim Auftragnehmer dar.

10.4 Der Auftragnehmer hat regelmäßig und bei gegebenem Anlass 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 DSGVO).

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

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

11.1 Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Abstimmung zu vernichten.

11.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12 Haftung

12.1 Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen Datenverarbeitung oder -nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich, soweit nicht der Auftragnehmer oder ein Unterauftragnehmer oder Mitarbeiter von diesen gegen seine/ihre Pflichten aus Gesetz oder aus diesem Vertrag bzw. dem Hauptvertrag verstoßen haben.

12.2 Die Vertragspartner stellen sich jeweils von der Haftung frei, wenn ein Vertragspartner nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

12.3 Der Auftragnehmer ist zum Zwecke der Enthaftung gem. Art. 82 Abs. 3 DSGVO dazu befugt, Details zu Weisungen des Auftraggebers und zur erfolgten Datenverarbeitung offenzulegen. Der Auftraggeber ist dazu verpflichtet, den Auftragnehmer bestmöglich zu unterstützen, damit sich der Auftragnehmer gegenüber dem Dritten nach Art. 82 Abs. 3 DSGVO enthaften kann.

12.4 Sofern gegen den Auftragnehmer ein Bußgeld aufgrund des Verstoßes gegen eine datenschutzrechtliche Verpflichtung, die ausschließlich den Auftraggeber trifft, verhängt wird, hat der Auftraggeber den Auftragnehmer freizustellen.

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

13 Sonstiges

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

13.2 Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, so wird dadurch die Gültigkeit dieser Vereinbarung im Übrigen nicht berührt. Die Vertragspartner werden in einem solchen Fall die unwirksame Bestimmung durch eine gesetzeskonforme Regelung ersetzen.

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 bereit gestellten Daten des Kunden zu nehmen. Der Zugriff erfolgt ausschließlich für den Zweck der Fehleranalyse und Fehlerbeseitigung.

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 DSGVO benannt		
Name:	Carola Sieling Technologiewerft GmbH, c/o Kanzlei Sieling	
Straße:	Gurlittstraße 24	
PLZ/Ort:	20099 Hamburg	
Telefon:	040/41923921	
E-Mail-Adresse:	info@technologiewerft.de	
Internet-Adresse:	www.technologiewerft.de	

6. Der Auftragnehmer verpflichtet sich, auch für diesen Auftrag relevante Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen. Der Auftragnehmer beachtet diese besonderen Regeln der Berufsgeheimnisträger und verpflichtet seine Mitarbeitenden entsprechend, (wie z. B. 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
Zammad GmbH Marienstraße 18 10117 Berlin	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	Zahlungsverkehr

24118 Kiel	
Canon Deutschland GmbH Europapark Fichtenhain A10 47807 Krefeld	Druckmaschinen-Hersteller
Reisswolf Akten und Datenvernichtung GmbH & Co. KG Wendenstraße 403 20537 Hamburg	Datenvernichtung
BÖWE SYSTEC GmbH Werner-von-Siemens Str. 1 86159 Augsburg	Kuvertiermaschinen-Hersteller
Bechtle IT-Systemhaus Hamburg Bernhard-Nocht-Straße 113 20359 Hamburg	Externer IT und Netzwerk Service
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen	Videokonferenzsoftware, Support
X KEY GmbH Gerstlgasse 30 1210 Wien Österreich	Support LXP TREIBER

Anlage 2

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 DSGVO)

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
☒ Alarmanlage
☒ Videoüberwachung
☒ Spezielle Schutzvorkehrungen des Serverraums
☒ Mitarbeiter- und Berechtigungsausweise
☒ Sperrbereiche

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)
☒ 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

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 externen Datenträgern und/oder Laptops (etwa per Betriebssystem, TrueCrypt, Safe Guard Easy, WinZip, PGP)
☒ Vier-Augen-Prinzip
☒ Aufgabentrennung
☒ Aufgabenbezogene Berechtigungsprofile
☒ Passwort-Identifikation, etc.

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

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
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 DSGVO)

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 externen Datenträgern und/oder Laptops (etwa per Betriebssystem, TrueCrypt, 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.

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

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

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 DSGVO);

Zweck:
Es muss sichergestellt sein, dass die personenbezogenen Daten nicht zufällig zerstört werden und vor Verlust ge-schützt 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.

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

Der Auftragsverarbeiter ist zertifiziert nach DIN ISO 27001;
Zertifikats-ID: DSC.897.07.2020, gültig bis 30.07.2023

Dieses beinhaltet ein nachgewiesenes:

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

Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO 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
☒ Regelmäßige Schulungen aller zugriffsberechtigten Mitarbeiter
☒ Regelmäßig stattfindende Nachschulungen
☒ Verpflichtung der Mitarbeiter auf die Vertraulichkeit gem. DSGVO
☒ Verpflichtung der Mitarbeiter auf das Sozialgeheimnis
☒ Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis
☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
☒ Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag
☒ Service Level Agreements (SLAs) für den Einsatz von Kontrollen