**Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO**

zwischen

| **Auftragsverarbeiter** | **Auftraggeber** |
|---|---|
| A & O GmbH | Name |
| Elisabeth-Selbert-Straße 5. | Strasse |
| 63110 Rodgau Dudenhofen | Ort |
| **(nachstehend A&O genannt)** | **(nachstehend Auftraggeber genannt)** |
| Rodgau, den | Ort/ Datum |
| Jens Kreis _____ | Name Unterschriftsberechtigter |
| **Weisungserhaltende A&O** | **Weisungsberechtigte Auftraggeber** |
| A&O Person1 | AG Person1 |
| A&O Person 2 | AG Person2 |
| **Datenschutzbeauftragter A&O**<br>Martin Bastian, Dadivo UG,<br>Schäfergasse 25, 63477 Maintal<br>Tel. 06109-7688938, Mail: bastian@dadivo.com | **Datenschutzbeauftragte(r)Auftraggeber**<br>Name<br>Kontaktdaten |

**1. Gegenstand und Dauer des Vertrags**

Verarbeitung von Adressdaten und anschließend Aufbringung auf Heft, Etikett oder Deckblatt zum Zweck der Postauslieferung oder Übergabe an andere Dienstleister der Verlage durch A&O.

Dies beinhaltet die Datenaufbereitung der Adressdaten für den Pressepost-, Infopost-, Auslands- und Paketversand. Erstellung der Versandpapiere. Versand der Pressepost und Dialogpost über die DPAG oder andere Zustelldienste.

Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung bzw. Hauptvertrag.

Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

**2. Art der Daten und Betroffener Personenkreis**

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

Adressdaten (Name, Anschrift, PLZ, Ort), Vertragsstammdaten (Abonnement /Auftragsnummer) Kommunikationsdaten (z.B. Telefon, E-Mail), Vertragsabrechnungs- und Zahlungsdaten.

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Aktive Abonnenten oder zum einmaligen Versand übergebene Werbeadressen der vom Auftraggeber betreuten Verlage, Kunden, Interessenten.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Jede Verlagerung 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.

**3. Technisch-organisatorische Maßnahmen**

(1) A&O hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Vertragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) A&O hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es A&O gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

**4. Rechte von betroffenen Personen**

(1) A&O unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an A&O wendet, wird A&O dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch A&O sicherzustellen.

**5. Qualitätssicherung und sonstige Pflichten von A&O**

(1) A&O hat zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. A&O setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. A&O

und jede A&O unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(b) Der Auftraggeber und A&O arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Zu diesem Zweck und um insbesondere die kurzen gesetzlichen Meldefristen bei Datenschutzverstößen einhalten zu können, teilt der Auftraggeber A&O die Kontaktdaten seines Datenschutzbeauftragten oder der verantwortlichen Stelle mit.

(c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei A&O ermittelt.

(d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei A&O ausgesetzt ist, hat ihn A&O nach besten Kräften zu unterstützen.

(e) A&O kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

(g) A&O meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

(h) A&O unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zu Verfügung.

(i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn A&O unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

**6. Unterauftragsverhältnisse**

(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 A&O in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung von A&O nach diesem Vertrag erbracht werden. A&O ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) A&O darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch A&O kontrolliert. A&O stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. A&O stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR stellt A&O die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

**7. Internationale Datentransfers**

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

- Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

oder

- Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland. In diesem Fall werden in Anlage 2 die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

**8. Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, in Absprache mit A&O Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch A&O in dessen Geschäftsbetrieb zu überzeugen.

(2) A&O stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten von A&O nach Art. 28 DS-GVO überzeugen kann. A&O verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

• die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

• die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

• aktuelle Testate, Berichte oder Berichtsauszüge

• unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

• eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann A&O einen Vergütungsanspruch geltend machen.

**9. Weisungsbefugnis des Auftraggebers**

(1) A&O verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(2) A&O hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. A&O ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

**10. Löschung und Rückgabe von personenbezogenen Daten**

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat A&O sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

**11. Haftung und Schadensersatz**

A&O und Auftraggeber haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

**12. Geheimhaltungspflichten**

(1) A&O und Auftraggeber verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

**13. Vergütung**

Regelungen zu einer Vergütung von Leistungen sind zwischen A&O und Auftraggeber gesondert zu vereinbaren.

**14. Schlussbestimmungen**

(1) Sollte eine Bestimmung dieser Vereinbarung ungültig oder nicht durchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieser Vereinbarung hiervon unberührt. Die Parteien vereinbaren, die ungültige oder nicht durchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das gleiche gilt im Falle einer Regelungslücke.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch A&O i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

Anlage 1 – Genehmigte Unterauftragsverarbeiter

Anlage 2 – Technisch-Organisatorische Maßnahmen

Anlage 1

**<u>Genehmigte Unterauftragnehmer A & O GmbH</u>**

- IT-Services – i.b.k.e. GmbH, Wiener Str. 120-124, 60599 Frankfurt am Main
- Software und Cloud-Dienste - Microsoft 365 - Microsoft Ireland Operations, Ltd. Attn: Data Privacy, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
- Aktenvernichtung - Jochen Westarp Data-Ex GmbH, Römerstraße 17, 63741 Aschaffenburg

Anlage 2

**A & O GmbH**
**Technisch-organisatorische Maßnahmen gem. Art. 32 DSGVO**
**Sicherheit der Verarbeitung**

**Zutrittskontrolle**

- Umzäuntes Firmengelände mit Metallzaun
- Personenkontrolle am Empfang
- Sicherheitsschließsystem mit abgestuften Berechtigungen
- Bürobereich im ersten Stock, Zugangsmöglichkeit nur über Treppenhaus
- Räumlich separierter Bürobereich und Serverraum
- Einbruchshemmende Zugangstüren zu Büros und Serverraum
- Externe Personen nur in Begleitung von A&O Mitarbeitern

**Zugangskontrolle**

- Anmeldung der MA an EDV-System mit Benutzername und Kennwort
- Passwortlänge mindestens 12 Zeichen (Buchstaben, Zahlen, Sonderzeichen)
- Passwörter dürfen nicht aus Namen, Vorname, Geburtsdaten oder geografischen Begriffen bestehen. Die Verwendung von Trivialpasswörtern ist untersagt.
- Passwortwechsel bei vermuteter Kompromittierung
- Unverzügliche Änderung von lnitialpasswörtern
- Automatische Bildschirmschoneraktivierung nach 15 Minuten
- Vorgeschriebenes Sperren des Computers beim Verlassen des Arbeitsplatzes
- Reaktivierung Bildschirmschoner nur durch Passworteingabe
- Firewall
- Zentral verwaltete Antivirensoftware (Client Security, Exchange, Fileserver)
- Signaturaktualisierung alle 60 Minuten
- Sicherheitssoftware mit Zugriffsrestriktionen nach Policies, mit Protokollierung und Logfilekontrolle
- Zentrales Endpoint Management
- Emailsystem verschlüsselt und Zertifikatsbasiert, Multifaktorauthentifizierung

**Zugriffskontrolle**

- Berechtigungssystem- Zugriff nur auf freigegebene Verzeichnisse bzw. über Policies
- WLAN WPA2-Verschlüsselt und MAC-Adressfilter, Protokollierung des Zugriffs
- VPN über SSTP und Zertifikat, Protokollierung
- Protokollierung der Systemanmeldungen, Kontrolle stichprobenartig.

**Weitergabekontrolle**

- Datenübertragung per SFTP-Server. Protokollierung
- Datenspeicherung auf eigene Server oder Cloud Dienstleistern, welche die DSGVO Vorgaben erfüllen
- VPN über SSTP und Zertifikat, Protokollierung
- Datenübermittlung an Dritte Unternehmen findet nicht statt.

**Eingabekontrolle**

- Protokolle der Verarbeitungsprozesse.
- Berechtigungskonzept zum Bearbeiten und Löschen von Daten.
- Aufbewahrung und Archivierung von Mails, Formularen oder Unterlagen.

**Auftragskontrolle**

- Verpflichtung der Mitarbeiter auf Verschwiegenheit
- Klare Weisungsbefugnisse an die Mitarbeiter im Umgang mit Kundendaten, auch spezifisch nach Kundenvorgabe.
- Vor-Ort Kontrollen und Stichproben.
- Regelmäßige Sensibilisierung und Unterweisung der Mitarbeiter im Datenschutzrecht und Datensicherheit

**Verfügbarkeitskontrolle**

- Tägliches Backup auf NAS. Zusätzliches Backup auf externe Medien und Aufbewahrung an anderem, abgesichertem Ort
- Konzept für Disaster-Recovery
- USV
- Brandschutz / Wasserschutzmaßnahmen
- Server RAID 10
- Klimaanlage
- Virenschutz

**Trennungsgebot**

- Verarbeitung von Kundendaten nach Kundenvereinbarung, getrennte Datenbanken, getrennte Ordnerstrukturen
- Fileserver, Auftragsverarbeitung, Buchhaltung, separate Server (Virtuelle Maschinen-VMWARE) ausgeführt
- Testsysteme sind getrennt von Produktivsystemen.

**Datenschutz-Management**

- Fortlaufende Überprüfung, Bewertung und Evaluierung von Schutz- und Sicherheitsmaßnahmen
- Bestellung eines externen Datenschutzbeauftragten (Martin Bastian - Dadivo UG)