



**VERTRAG  
ZUR AUFTRAGSVERARBEITUNG GEMÄSS ART. 28 DSGVO  
FÜR IT-ENTERPRISE-SERVICES**

Kunde: \_\_\_\_\_

Person: \_\_\_\_\_

\_\_\_\_\_

E-Mail: \_\_\_\_\_

Adresse: \_\_\_\_\_

Telefon: \_\_\_\_\_

\_\_\_\_\_

Fax: \_\_\_\_\_

\_\_\_\_\_

Stichtag: \_\_\_\_\_

Kundennummer: \_\_\_\_\_

Dieser Vertrag basiert auf dem Vertragsvorschlag der *Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)* und wurde auf die Anforderungen von Knipp entsprechend angepasst.

Dieser Vertrag wird zum oben genannten Stichtag geschlossen. Die Vertragsparteien sind der oben genannte Kunde (nachfolgend *Kunde* genannt) und Knipp Medien und Kommunikation GmbH (nachfolgend *Knipp* genannt, dem Lieferanten), der seinen Sitz im Martin-Schmeißer-Weg 9, Technologiepark, Dortmund, Deutschland hat und für sich und seine Tochtergesellschaften handelt.

## 1. DEFINITIONEN

1.1 **Verantwortlicher** bedeutet in diesem Zusammenhang Kunde.

1.2 **Verarbeiter** bedeutet Knipp als Lieferant der Dienstleistungen.

## 2. GEGENSTAND UND DAUER DES VERTRAGS

2.1 Der **Gegenstand** des Vertrags ergibt sich aus dem gesonderten Leistungsvertrag inklusive eventueller Aktualisierungen.

2.2 Die **Dauer** des Vertrags ergibt sich aus dem gesonderten Leistungsvertrag inklusive eventueller Aktualisierungen.

## 3. KONKRETISIERUNG DES VERTRAGSINHALTS

3.1 Die **nähere Beschreibung** des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben ergeben sich aus dem gesonderten Leistungsvertrag inklusive eventueller Aktualisierungen. Dabei erbringt Knipp Wartungsarbeiten an technischen Systemen (z.B. Erstellung von Datensicherungen) und hat dadurch eventuell auch Zugang zu personenbezogenen Daten. Darüberhinaus können auch E-Mail-Konten verwaltet werden. 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. DSGVO erfüllt sind. Das angemessene Schutzniveau ist festgestellt durch ei-

nen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO).

3.2 Der **Gegenstand** der Verarbeitung personenbezogener Daten hängt von den Applikationen ab, die der Verantwortliche auf dem System pflegt. Knipp hat keine Kenntnisse über Art und Umfang der Daten.

## 4. TECHNISCH-ORGANISATORISCHE MASSNAHMEN

4.1 **Dokumentation.** Der Verarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

4.2 **Sicherheit.** Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen [Einzelheiten in Anhang A].

4.3 Die **technischen und organisatorischen Maßnahmen** unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

## 5. BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN

5.1 Der Auftragnehmer darf die Daten, die im Auftrag ver-

arbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 6. QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS

6.1 **Datenschutzbeauftragter.** Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

6.2 Die Wahrung der **Vertraulichkeit** gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer 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. Der Auftragnehmer und jede dem Auftragnehmer 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.

6.3 **TOMs.** Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anhang A].

6.4 **Zusammenarbeit.** Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

6.5 **Inspektionen.** Die unverzügliche Information des Auftraggebers 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 Auftragnehmer ermittelt.

6.6 **Aufsichtsbehörden.** 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 beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

6.7 **Regelmäßige Kontrolle.** Der Auftragnehmer 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.

6.8 **Nachweisbarkeit** der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## 7. UNTERAUFTRAGSVERHÄLTNISSE

7.1 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. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

7.2 **Zustimmung.** Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

## 8. KONTROLLRECHTE DES AUFTRAGGEBERS

8.1 **Inspektionen.** Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer 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 den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

8.2 **Auskünfte.** Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

8.3 Der **Nachweis** solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- (a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- (b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- (c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- (d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz oder ISO/IEC 27001).

8.4 **Vergütung.** Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

## 9. MITTEILUNG BEI VERSTÖßEN DES AUFTRAGNEHMERS

9.1 **Unterstützung.** Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:

- (a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognosti-

zierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

(b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.

(c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

(d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

(e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

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

## 10. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

10.1 **Bestätigungen.** Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

10.2 **Rechtsverstöße.** Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 11. LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

11.1 **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.

11.2 **Rückgabe von Unterlagen.** Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer 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.

11.3 **Vertragsdauer.** 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.

**Ordnungsgemäß bevollmächtigte Vertreter** der Vertragsparteien:

**Knipp Medien und Kommunikation GmbH**

**Kunde**

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Funktion: \_\_\_\_\_

Funktion: \_\_\_\_\_

Datum: \_\_\_\_\_

Datum: \_\_\_\_\_

Unterschrift: \_\_\_\_\_

Unterschrift: \_\_\_\_\_

## Anhang A

## TECHNISCH-ORGANISATORISCHE MASSNAHMEN

**A.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)****A.1.1 Zutrittskontrolle**

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen;

**A.1.2 Zugangskontrolle**

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

**A.1.3 Zugriffskontrolle**

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

**A.1.4 Trennungskontrolle**

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

**A.1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)**

Die Verarbeitung personenbezogener Daten 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;

**A.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)****A.2.1 Weitergabekontrolle**

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

**A.2.2 Eingabekontrolle**

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

**A.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)****A.3.1 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;

**A.3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);****A.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DS-GVO)****A.4.1 Datenschutz-Management;****A.4.2 Incident-Response-Management;****A.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);****A.4.4 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.