Allgemeine Geschäftsbedingungen der A1 Digital Deutschland GmbH für Auftragsverarbeitung (AGB AVV)

V2.0, Gültig ab Juli 2023
Autor: A1 Digital Deutschland Data Privacy Officer

1. Geltungsbereich, Gegenstand und Dauer des Auftrags

(1) Diese AGB AVV sind die Vertragsgrundlage für bestehende und zukünftige Vertragsbeziehungen zwischen der A1 Digital Deutschland GmbH („A1 Digital") und Kunden von A1 Digital, soweit A1 Digital im Rahmen von Vertragsbeziehungen zu Kunden (im Folgenden auch „Auftraggeber") personenbezogene Daten in deren Auftrag als Auftragsverarbeiter nach Art 28 EU-DSGVO verarbeitet; sie gelten insbesondere für alle Datacenter-, Applications- Service und Supportleistungen, die von A1 Digital erbracht werden, soweit dabei personenbezogene Daten von Kunden von A1 Digital verarbeiten werden.

(2) Der Gegenstand des Auftrags ergibt sich aus dem jeweiligen Vertragsverhältnis (im Folgenden „Leistungsvereinbarung"), das Rechtsgrundlage für die Durchführung von Datenverarbeitungen durch den Auftragsverarbeiter ist.

(3) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der jeweiligen Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der Verarbeitung, die Kategorien der betroffenen Personen sowie die Art der personenbezogener Daten sind konkret beschrieben in der jeweiligen Leistungsvereinbarung samt Anhang zum Datenschutz.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung durch Übermittlung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in diesem Drittland ist entweder

a) festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO); oder
b) wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO); oder
c) wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DS-GVO); oder
d) wird hergestellt durch genehmigte Verhaltensregeln (Art 46 Abs. 2 lit. e i.V.m. 40 DS-GVO); oder
e) wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO); oder
f) wird hergestellt durch sonstige Maßnahmen (Art. 46 Abs 2 lit. a, Abs. 3 lit. a und b DS-GVO).

Liegt keine dieser Voraussetzungen vor, ist eine Datenverarbeitung im Drittland nicht zulässig.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter 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.

(2) Der Auftragsverarbeiter hat die Sicherheit gemäß 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 zur 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. Sofern in der Leistungsvereinbarung nicht genauer geregelt, obliegt es dem Auftragsverarbeiter, das der jeweiligen Verarbeitung angemessene Schutzniveau insbesondere durch eine Kombination von den in Anlage 1 genannten technisch-organisatorischen Maßnahmen sicherzustellen. Es ist dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

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

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Verantwortlichen unverzüglich mitgeteilt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Leistungsvereinbarung, bzw. der Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO .
d) Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Sofern gesetzlich zulässig, die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Der Auftragsverarbeiter wird in diesem Fall die Behörde an den Verantwortlichen verweisen.

f) Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.
g) Der Auftragsverarbeiter 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 Personen gewährleistet wird.
h) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

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

(2) Soweit nicht bereits in der Leistungsvereinbarung festgelegt, kann der Auftragsverarbeiter weitere Unterauftragsverarbeiter (autorisierte Personen) zur Unterstützung der Datenverarbeitung gemäß dieser Vereinbarung in Anspruch nehmen. Es wird vereinbart, dass die zum Zeitpunkt des Abschlusses der Leistungsvereinbarung eingesetzten Unterauftragsverarbeiter als genehmigte Unterauftragsverarbeiter gelten. Der Auftragsverarbeiter wird den Verantwortlichen so rechtzeitig über einen Wechsel des Unterauftragnehmers schriftlich informieren, dass der Verantwortliche dies allenfalls unter Angabe eines sachlichen Grundes untersagen kann. Sofern ein konzernverbundenes Unternehmen als Unterauftragsverarbeiter herangezogen wird, gilt die Zustimmung des Verantwortlichen als erteilt.

(3) Alle Unterauftragsverarbeiter unterliegen den gleichen Verpflichtungen wie der Auftragsverarbeiter im Rahmen dieser Vereinbarung bzw. mit dieser Vereinbarung zusammenhängenden Vereinbarungen.

(4) Der Auftragsverarbeiter ist jederzeit gegenüber dem Verantwortlichen zur Einhaltung dieser Vereinbarung und damit im Zusammenhang stehenden Vereinbarungen durch die Unterauftragsverarbeiter verantwortlich.

7. Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

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

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
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);
e) Jahresberichte durch den Auftragsverarbeiter.

(3) Sofern darüberhinausgehende Informationen vom Verantwortlichen benötigt werden, um seinen eigenen Audit Verpflichtungen nachzukommen oder wenn seitens der zuständigen Behörde ein entsprechender Auftrag vorliegt, wird der Verantwortliche den Auftragsverarbeiter schriftlich davon in Kenntnis setzen, sodass dieser diese Informationen liefern kann bzw. dem Verantwortlichen Zugang zu den Informationen einräumen kann.

(4) Sofern die oben angeführten Informationen nicht ausreichend erachtet werden, um die Audit Verpflichtung gemäß dem anwendbaren Recht zu erfüllen, oder wenn eine materielle Datenschutzverletzung stattgefunden hat, für die den Auftragsverarbeiter eine Verantwortung trifft, hat der Verantwortliche das Recht, im Einvernehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die einen Monat im Vorhinein anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

(5) Um eine Überprüfung durchzuführen, sendet der Verantwortliche einen detaillierten Audit-/Kontroll-Plan mindestens zwei Wochen vor dem geplanten Prüfungstermin an den Auftragsverarbeiter und gibt darin den Umfang, die Dauer der Überprüfung sowie das Startdatum der Prüfung bekannt. Der Auftragsverarbeiter überprüft den Audit-/Kontroll-Plan und übermittelt an den Verantwortlichen hierzu alle wesentlichen Bedenken und Fragen, wie beispielsweise Anfragen zu Informationen, die die Sicherheit, Privatsphäre oder Beschäftigungspolitik des Auftragsverarbeiters beeinträchtigen können. In jedem Fall arbeitet der Auftragsverarbeiter mit dem Verantwortlichen kooperativ zusammen, um einen abschließenden Audit-/Kontroll-Plan zu vereinbaren.

(6) Die Überprüfung findet während der regulären Geschäftszeiten, gemäß den Betriebsrichtlinien der jeweiligen Betriebsstätte des Auftragsverarbeiters statt und darf den Betrieb des Auftragsverarbeiters nicht unangemessen beeinträchtigen. Der Auftragsverarbeiter strengt sich angemessen an, um dem Prüfer die angeforderten Informationen zur Verfügung zu stellen.

(7) Der Verantwortliche trägt die Kosten für die Durchführung der Kontrollen selbst. Für weitergehende Unterstützungsleistungen kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen. Hierfür legt der Auftragsverarbeiter ein Angebot, welches einvernehmlich abzustimmen ist.

8. Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO 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 prognostizierte 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 Verantwortlichen zu melden;
c) die Verpflichtung, dem Verantwortlichen 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 Verantwortlichen für dessen Datenschutz-Folgenabschätzung;
e) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten, oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen, die einvernehmlich zu vereinbaren ist.

9. Weisungsbefugnis des Verantwortlichen

(1) Zusätzlich zu den vertraglich vereinbarten Vorgaben können schriftliche Weisungen vom Verantwortlichen auch per E-Mail (in Textform) erteilt werden.

(2) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen 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 Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen und 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 den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

11. Anwendbares Recht und Gerichtsstand

Diese Vereinbarung unterliegt ausschließlich dem deutschen Recht mit Ausschluss der Anwendung der Kollisionsbestimmungen des internationalen Privatrechtes. Alle Streitigkeiten aus oder in Zusammenhang mit dieser Vereinbarung sind ausschließlich vom sachlich zuständigen Landgericht München I, zu entscheiden.

Anlage – Technisch-organisatorische Maßnahmen

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

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  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;

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

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);

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

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