

# Auftragsverarbeitungsvertrag

**Gemäß Art. 28 Abs. 3 S. 1 DSGVO – nachstehend bezeichnet als AV-Vertrag –**

zwischen

Kunden der IT-Service, Kunadt & Gleditzsch GbR

– nachstehend bezeichnet als **Auftraggeber** –

und der

IT-Service, Kunadt & Gleditzsch GbR

– nachstehend bezeichnet als **Auftragnehmer** –

– Auftragnehmer und Auftraggeber werden nachstehend auch als **Vertragsparteien** bezeichnet. –

---

## Anlagen

- [Anhang 1 "Sicherheitskonzept"](#)

---

### 1. **Gegenstand des Auftrags, Datenkategorien, Betroffene, Art, Umfang und Zwecksetzung der Verarbeitung (Art. 28 Abs. 3, 30 Abs. 2 DSGVO)**

1. Der Gegenstand des AV-Vertrages, die im Rahmen des Auftrags verarbeiteten personenbezogenen Daten (Art, 4 Nr. 1 DSGVO; nachfolgend kurz „Daten“), die von der Verarbeitung betroffene Personen (nachfolgend kurz „Betroffene“) sowie Art, Umfang und Zwecke der Verarbeitung, werden durch die folgenden Rechtsbeziehung(en) zwischen den Vertragsparteien bestimmt (nachstehend bezeichnet als Hauptvertrag):

Die Vertragsparteien arbeiten auf Grundlage einzelner Aufträge, die der Auftraggeber gegenüber dem Auftragnehmer erteilt, bzw. im Rahmen einzelner Verträge, die der Auftraggeber mit dem Auftragnehmer schließt, zusammen.

Die Regelungen dieses AV-Vertrages gelten gegenüber dem Hauptvertrag vorrangig.

2. Art der Daten:

- Bestandsdaten (z.B., Namen, Adressen).
- Kontaktdaten (z.B., E-Mail, Telefonnummern).
- Vertragsdaten (z.B., Vertragsgegenstand, Laufzeit).

3. Verarbeitung besonderer Kategorien von Daten (Art. 9 Abs. 1 DSGVO):
4. Kategorien der Betroffenen
5. Zweck der Verarbeitung:
2. Verantwortlichkeit und Weisungsrecht
  1. Der Auftraggeber ist als Verantwortlicher gem. Art. 4 Nr. 7 DSGVO für die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere für die Auswahl des Auftragnehmers, die an diesen übermittelten Daten sowie erteilte Weisungen verantwortlich (Art. 28 Abs. 3 lit. a, 29 u. 32 Abs. 4 DSGVO).
  2. Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrages sowie der Weisungen des Auftraggebers verarbeiten (was insbesondere auch für deren Berichtigung, Löschung oder Einschränkung der Verarbeitung gilt) und nur insoweit die Verarbeitung hierzu erforderlich ist, außer wenn der Auftragnehmer zu der Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber 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 S. 2 lit. a DSGVO).
  3. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen im Hinblick auf die Verarbeitung der Daten und die Sicherheitsmaßnahmen zu erteilen.
  4. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber unverzüglich darauf hinweisen. In diesem Fall ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zur Bestätigung der Weisung durch den Auftraggeber auszusetzen und im Fall offensichtlich rechtswidriger Weisungen abzulehnen.
  5. Gehen ergänzende Weisungen des Auftraggebers über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem Fehlverhalten des Auftragnehmers, dann hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.
  6. Die Vertragsparteien können zum Erteilen und Empfangen von Weisungen berechnete Personen benennen (insbesondere, wenn diese sich nicht bereits aus dem Hauptvertrag ergeben) und sind verpflichtet deren Änderung unverzüglich mitzuteilen.
3. Sicherheitskonzept und diesbezügliche Pflichten
  1. Der Auftragnehmer wird die innerbetriebliche Organisation in seinem Verantwortungsbereich entsprechend den gesetzlichen Anforderungen gestalten und wird insbesondere technische und organisatorische Maßnahmen (nachfolgend bezeichnet als „TOMs“) zur angemessenen Sicherung, insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit von Daten des Auftraggebers, unter Beachtung des Stands der Technik, der

Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen treffen sowie deren Aufrechterhaltung sicherstellen (Art. 28 Abs. 3 u. 32 - 39 i.V.m. Art 5 DSGVO). Zu den TOMs gehören insbesondere die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle und die Sicherung der Betroffenenrechte.

2. Die diesem AV-Vertrag zugrundeliegenden TOMs ergeben sich aus dem Anhang 1 „Sicherheitskonzept“. Sie dürfen entsprechend dem technischen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden.
  3. Der Auftragnehmer stellt sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen auf Vertraulichkeit und Verschwiegenheit (Art. 28 Abs. 3 S. 2 lit. b und 29, 32 Abs. 4 DSGVO) verpflichtet und in die Schutzbestimmungen der DSGVO eingewiesen worden sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
  4. Die im Rahmen des AV-Vertrages überlassene Daten sowie Datenträger und sämtliche hiervon gefertigten Kopien verbleiben im Eigentum des Auftraggebers, sind durch den Auftragnehmer sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers, und dann nur datenschutzgerecht, vernichtet werden. Kopien von Daten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten des Auftragnehmers gegenüber dem Auftraggeber erforderlich sind (z.B. Backups).
  5. Sofern durch die DSGVO oder ergänzende, insbesondere nationale Vorschriften, vorgegeben, benennt der Auftragnehmer eine/n den gesetzlichen Vorgaben entsprechende/n Datenschutzbeauftragte/n und informiert den Auftraggeber entsprechend (Art. 37 bis 39 DSGVO).
4. Informationspflichten und Mitwirkungspflichten
1. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen, wobei der Auftragnehmer den Auftraggeber hierbei gem. Art. 28 Abs. 3 S. 2 lit. e. DSGVO unterstützt und ihn insbesondere über die bei ihm eingehenden Anfragen Betroffener informiert.
  2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung der Daten Fehler oder Unregelmäßigkeiten im Hinblick auf die Einhaltung der Bestimmungen dieses AV-Vertrages oder einschlägiger Datenschutzvorschriften feststellt.

3. Für den Fall, dass der Auftragnehmer Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der für den Auftraggeber verarbeiteten Daten verletzt worden ist, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen, und bei der Erfüllung der dem Auftraggeber obliegenden Pflichten gem. Art. 33 und 34 DSGVO zu unterstützen.
  4. Sollte die Sicherheit der Daten des Auftraggebers durch Maßnahmen Dritter (z.B. Gläubiger, Behörden, Gerichte, etc.) gefährdet sein (Pfändung, Beschlagnahme, Insolvenzverfahren, etc.) wird der Auftragnehmer die Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Auftraggeber liegen und nach Rücksprache mit dem Auftraggeber, sofern erforderlich, entsprechende Schutzmaßnahmen ergreifen (z.B. Widersprüche, Anträge, etc. stellen).
  5. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber dem Auftragnehmer tätig wird und deren Tätigkeit die für den Auftragnehmer verarbeiteten Daten betreffen kann. Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrnehmung seiner Pflichten (insbesondere zur Auskunfts- und Duldung von Kontrollen) gegenüber Aufsichtsbehörden (Art. 31 DSGVO).
  6. Der Auftragnehmer stellt dem Auftraggeber Informationen betreffend die Verarbeitung von Daten im Rahmen dieses AV-Vertrages, die für dessen Erfüllung von gesetzlichen Pflichten (zu denen insbesondere Anfragen Betroffener oder Behörden und die Einhaltung seiner Rechenschaftspflichten gem. Art. 5 Abs. 2 DSGVO, als auch die Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO gehören können) notwendig sind, zur Verfügung, sofern der Auftraggeber diese Informationen nicht selbst beschaffen kann. Die Informationen müssen dem Auftragnehmer zur Verfügung stehen und müssen nicht von Dritten beschafft werden, wobei Mitarbeiter, Beauftragte und Subunternehmer des Auftraggebers nicht als Dritte gelten.
  7. Gehen die Zurverfügungstellung der notwendigen Informationen und die Mitwirkung über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruht nicht auf einem Fehlverhalten des Auftragnehmers, hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.
5. Verarbeitung in Drittländern
    1. 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 (EWR) statt.

6. Dauer des Auftrags, Vertragsbeendigung und Datenlöschung
  1. Dieser AV-Vertrag wird mit dessen Abschluss gültig, wird auf unbestimmte Zeit geschlossen und endet spätestens mit der Laufzeit des Hauptvertrags.
  2. Das Recht auf außerordentliche Kündigung bleibt den Vertragsparteien vorbehalten, insbesondere im Fall eines schwerwiegenden Verstoßes gegen die Vorgaben dieses AV-Vertrages und geltendes Datenschutzrecht. Der außerordentlichen Kündigung hat grundsätzlich eine Abmahnung der Verstöße mit angemessener Frist voranzugehen, wobei sie nicht erforderlich ist, wenn nicht damit zu rechnen ist, dass die beanstandeten Verstöße behoben werden oder diese derart schwer wiegen, dass ein Festhalten am AV-Vertrag der kündigenden Vertragspartei nicht zuzumuten ist.
  3. Nach Abschluss der Erbringung der Verarbeitungsleistungen im Rahmen dieses AV-Vertrages, wird der Auftragnehmer alle personenbezogenen Daten und deren Kopien (sowie sämtliche im Zusammenhang mit dem Auftragsverhältnis in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände), nach Wahl des Auftraggebers entweder löschen oder zurückgeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 1 S. 2 lit. g DSGVO). Die Einrede eines Zurückbehaltungsrechts, wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Im Hinblick auf die Löschung oder Rückgabe, gelten die Auskunfts-, Nachweis und Kontrollrechte des Auftraggebers entsprechend diesem AV-Vertrag.
  4. Im Übrigen bleiben die Verpflichtungen aus diesem AV-Vertrag im Hinblick auf die im Auftrag verarbeiteten Daten auch nach Beendigung des AV-Vertrages bestehen.
  5. Gehen die Löschung, bzw. die Rückgabe der Daten über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem Fehlverhalten des Auftragnehmers, dann hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.
7. Haftung
  1. für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.
  2. Die Vertragsparteien stellen sich jeweils von der Haftung frei, wenn eine der Vertragsparteien nachweist, dass sie für den

Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, in keinerlei Hinsicht verantwortlich ist.

8. Schlussbestimmungen, Rangfolge, Änderungen, Kommunikationsform, Rechtswahl, Gerichtsstand
  1. Änderungen, Nebenabreden und Ergänzungen dieses AV-Vertrages und seiner Anhänge bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses AV-Vertrages handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
  2. Dieser AV-Vertrag verpflichtet den Auftragnehmer nur insoweit, als dies zur Erfüllung der gesetzlichen Pflichten, insbesondere nach Art. 28 ff. DSGVO erforderlich ist und legt dem Auftragnehmer darüber hinaus keine weiteren Pflichten auf.
  3. Vorbehaltlich einer Verpflichtung zur Schriftform in diesem AV-Vertrag und im Hauptvertrag, erfolgt die Kommunikation zwischen dem Auftragnehmer und Auftraggeber im Rahmen dieses AV-Vertrages (insbesondere im Hinblick auf Weisungen und Informationserteilung) zumindest in Textform (z.B. E-Mail). Eine geringere Form (z.B. mündlich) kann den Umständen nach statt der Textform zulässig sein (z.B. in Notfallsituation), muss jedoch unverzüglich zumindest in Textform bestätigt werden. Sofern die Schriftform verlangt wird, ist die Schriftform im Sinne der DSGVO gemeint.

---

## **Auftrag zur Verarbeitung personenbezogener Daten**

### **Anhang 1 – Sicherheitskonzept**

Technische und Organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogenen und mindestens halbjährlichen evaluiert wird.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerruf & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen

und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.

- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen
  - Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
  - Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virens Scanner und Firewalls.
  - Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.
  - Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebensächlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.
  - Zutrittskontrolle
    - Zutrittsregelungen für betriebsfremde Personen
  - Zugangskontrolle / Zugriffskontrolle
    - Firewalls (Hardware/Software).
    - Stets aktueller Virenschutz.
    - Stets aktuelle Softwareversionen.
    - Berechtigungs-/ Authentifizierungskonzepte mit auf Nötigste beschränkten Zugriffsregulierungen.
    - Ordnungsgemäße Vernichtung von Datenträgern.
  - Weitergabekontrolle
  - Eingabekontrolle
  - Auftragskontrolle
  - Verfügbarkeitskontrolle/ Integrität
  - Gewährleistung des Zweckbindungs-/Trennungsgebotes
    - Physische Mandantentrennung (hardwareseitig).
-