

Auftragsverarbeitungsvereinbarung

Allgemeine Vertragsbedingungen zur Auftragsverarbeitung nach Art. 28 DSGVO

Auftragnehmer	Steffen Grell - Lager im Griff Clemensstr. 54 53225 Bonn
---------------	--

Teil 2 der Allgemeinen Geschäftsbedingungen
Stand: August 2026
Veröffentlicht unter: <https://lagerimgriff.de/agb/>

1. Allgemeine Bestimmungen und Vertragsgegenstand

1.1 Der Auftragnehmer stellt seinen Kunden (nachfolgend „Auftraggeber“) die in der nachfolgenden Tabelle beschriebenen Leistungen zur Verfügung. Hierbei verarbeitet der Auftragnehmer u. a. personenbezogene Daten von Dritten (Drittdata) im Auftrag des Auftraggebers. Für die Verarbeitung dieser Drittdata gelten die vorliegenden Allgemeinen Vertragsbedingungen zur Auftragsverarbeitung (nachfolgend „AVV“).

Leistungen, bei denen Daten im Auftrag verarbeitet werden	Verarbeitete Datenarten	Betroffene Personenkategorien
Lagerverwaltung über Software	Name, Vorname, berufliche E-Mail-Adresse, berufliche Telefonnummer	Nutzungsberechtigte, Ansprechpartner von Kunden und Lieferanten des Auftraggebers
Online-Schulung	Name, Vorname, berufliche E-Mail-Adresse, berufliche Telefonnummer	Mitarbeitende beim Auftraggeber
Support	Name, Vorname, berufliche E-Mail-Adresse, Inhalt der Supportanfrage, berufliche Telefonnummer	Mitarbeitende beim Auftraggeber

1.2 Die Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Eine Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers. Betroffen ist derzeit allein der Versand von Push-Nachrichten über den in der Liste nach Ziff. 8.1 aufgeführten Subunternehmer Google Ireland Limited; dabei kann es zu einer Übermittlung an Google LLC in die Vereinigten Staaten kommen. Grundlage dieser Übermittlung ist der Angemessenheitsbeschluss der Europäischen Kommission zum EU-US Data Privacy Framework; entfällt er, gelten die mit Google vereinbarten Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO. Die Funktion ist standardmäßig deaktiviert; ob sie eingesetzt wird, entscheidet der Auftraggeber durch Aktivierung in den Einstellungen der Software.

2. Laufzeit und Kündigung

Die Laufzeit der Auftragsverarbeitung richtet sich nach der Laufzeit des Hauptvertrags. Soweit und solange nach Beendigung des Hauptvertrags personenbezogene Daten des Auftraggebers im Auftrag weiterverarbeitet werden, gilt diese Vereinbarung bis zu dem Zeitpunkt, zu dem die Verarbeitung dieser Daten durch die Auftragnehmer endet. Das Recht auf außerordentliche fristlose Kündigung aus wichtigem Grund bleibt hiervon unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragnehmer zu. Auftragnehmer informiert den Auftraggeber unverzüglich, falls Auftragnehmer der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit Auftragnehmer substantiiert anzweifelt, ist Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass Auftragnehmer durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden.

3.2 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine Weisung in Textform erfolgen konnte. Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig, im erforderlichen Umfang, zu kontrollieren. Auftragnehmer hat diese Überprüfungen - einschließlich Inspektionen - die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und zu diesen beizutragen.

4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und nicht zu einer übermäßigen Beeinträchtigung des Geschäftsbetriebs führen. In der Regel soll eine Prüfung nur nach vorheriger Anmeldung erfolgen, es sei denn, die vorherige Anmeldung würde den Kontrollzweck gefährden. Wenn der Auftraggeber einen Prüfer bestellt, darf dieser nicht im unmittelbaren Wettbewerbsverhältnis zu Auftragnehmer stehen.

4.3 Die Ergebnisse der Kontrollen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

4.4 Auftragnehmer verpflichtet sich, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Verpflichtungen zur Verfügung zu stellen.

5. Allgemeine Pflichten von Auftragnehmer

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2 Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 1 dieser AVV festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt. Auftragnehmer wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen.

7. Unterstützungspflichten von Auftragnehmer

Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 - 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 - 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die Auftragnehmer zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Auftragnehmer ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Die jeweils eingesetzten Subunternehmer sind abschließend in einer laufend aktualisierten Liste unter <https://lagerimgriff.de/subunternehmer/> veröffentlicht. Für die dort zum Zeitpunkt des Vertragsschlusses aufgeführten Subunternehmer gilt die Zustimmung mit Vereinbarung dieser AVV als erteilt. Auftragnehmer zeigt jede Änderung der Liste dem Auftraggeber zusätzlich nach Maßgabe von Ziff. 8.2 per E-Mail an die vom Auftraggeber hinterlegte Adresse an; die Veröffentlichung allein ersetzt diese Anzeige nicht. Ergänzend kann der Auftraggeber unter der genannten Adresse Änderungsbenachrichtigungen abonnieren.

8.2 Beabsichtigt Auftragnehmer den Einsatz weiterer Subunternehmer, wird Auftragnehmer dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des / der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des / der Subunternehmer(s) als genehmigt. In dringenden Fällen (z.B. bei kurzfristig benötigten Fehleranalysen oder Mängelbeseitigungen) kann Auftragnehmer die Anzeigefrist nach Satz 1 und die Widerspruchsfrist nach Satz 2 auf jeweils sieben Kalendertage verkürzen. Erfolgt ein fristgerechter Widerspruch, dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und / oder sonstige berechnigte Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen.

8.3 Subunternehmer werden von Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter (Auftragnehmer) und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche Auftragnehmer zur Ausübung von geschäftlichen Tätigkeiten in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung sowie Post- und Transportdienstleistungen. Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

8.4 Sämtliche Verträge zwischen Auftragnehmer und dem Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieser AVV und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.

8.5 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten von Auftragnehmer

9.1 Verstöße gegen diese AVV, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer bei Auftragnehmer angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die Auftragnehmer zur Erfüllung vertraglicher Pflichten eingesetzt hat, begangen wurde.

9.2 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter Auftragnehmer um Auskunft, Berichtigung oder Löschung von Daten, die Auftragnehmer als Auftragsverarbeiter verarbeitet, wird Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten und das weitere Vorgehen mit ihm abstimmen.

9.3 Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von denen auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung des Hauptvertrags hat Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine rechtliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen).

11. Datengeheimnis und Vertraulichkeit

Auftragnehmer ist unbefristet und über das Ende des Hauptvertrags hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. Auftragnehmer verpflichtet sich, Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit bei Auftragnehmer aufnehmen.

12. Schlussbestimmungen

12.1 Sind die Vertragsparteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist der Sitz von Auftragnehmer Gerichtsstand für alle Streitigkeiten aus diesen AVV, sofern insoweit hierfür ein ausschließlicher Gerichtsstand nicht begründet wird.

12.2 Soweit personenbezogene Daten im Auftrag betroffen sind, gehen die Regelungen dieser AVV gegenüber den Regelungen der Hauptvereinbarung vor.

12.3 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.4 Auftragnehmer ist berechtigt, die vorliegenden AVV aus sachlich gerechtfertigten Gründen (z.B. Änderungen in der Rechtsprechung, Gesetzeslage, Marktgegebenheiten oder der Geschäfts- oder Unternehmensstrategie) und unter Einhaltung einer angemessenen Frist zu ändern. Bestandskunden werden hierüber spätestens zwei Wochen vor Inkrafttreten der Änderung per E-Mail benachrichtigt. Sofern der Bestandskunde nicht innerhalb der in der Änderungsmitteilung gesetzten Frist widerspricht, gilt seine Zustimmung zur Änderung als erteilt. Im Falle des Widerspruchs ist Auftragnehmer berechtigt, den Vertrag zum Zeitpunkt des Inkrafttretens der Änderung außerordentlich zu kündigen. Die Benachrichtigung über die beabsichtigte Änderung dieser AVV wird auf die Frist und die Folgen des Widerspruchs oder seines Ausbleibens hinweisen.

Anlage 1 - Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt. Soweit sich Maßnahmen auf Rechenzentren und Serverräume beziehen, werden sie von den in der Subunternehmerliste aufgeführten Hosting-Dienstleistern in deren Rechenzentren erbracht; der Auftragnehmer betreibt keine eigenen Serverräume.

1. Sicherung der Arbeitsstätte des Auftragsverarbeiters (Zutrittskontrolle)

- Schlüsselregelung
- Manuelles Schließsystem
- System für Zutrittsberechtigungen für Mitarbeiter und Dritte
- Sorgfältige Auswahl von Hilfspersonal (z. B. Reinigungskräfte)

2. Sicherung der IT-Systeme des Auftragsverarbeiters (Zugangskontrolle)

- Erstellung und Verwendung von Benutzerprofilen auf Personenebene
- Zuordnung von Benutzerrechten
- Passwortrichtlinie inkl. Mindestlänge, Wechselintervall, Mindestanforderungen an Passwörter
- Authentifizierung mit persönlicher Benutzerkennung und Passwort
- Einsatz einer dem Stand der Technik entsprechenden Software-Firewall
- Einsatz einer dem Stand der Technik entsprechenden Anti-Viren-Software
- Automatische Bildschirmsperre
- Differenziertes Berechtigungskonzept, Freigabe der Daten nur für Befugte
- Verwaltung der Zugriffsrechte durch Administrator; Anzahl der Administratoren minimiert
- Zeitnahe Sperrung der Konten ausgeschiedener Mitarbeiter
- Richtlinie zu Eingabe und Erfassung von Daten

3. Protokollierung von Datenverarbeitungsprozessen (Eingabekontrolle)

- Protokollierung von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines detaillierten Berechtigungskonzepts
- Protokollierung der Eingabe

4. Sichere Löschung von Daten

- Löschung von Datenträgern nach Verwendung
- Einsatz von Aktenvernichtern

5. Datenschutz bei den Subunternehmern des Auftragnehmers

- Vertragliche Regelung der Zusammenarbeit zwischen Auftragnehmer und Unterauftragsverarbeiter
- Sorgfältige Auswahl von Auftragsverarbeitern
- Prüfung der technischen und organisatorischen Maßnahmen der eingesetzten Subunternehmer anhand deren Dokumentation nach Art. 32 DSGVO

6. Sicherung von Daten bei Transport und Übermittlung (Weitergabekontrolle)

- Verschlüsselte Datenübertragungen
- Weitergabe von Daten an Dritte ist untersagt
- Dokumentation der Empfänger und ggf. der Zeitspannen von geplanten Überlassungen bzw. vereinbarter Löschfristen

7. Datensicherung und Backups (Verfügbarkeit und Wiederherstellbarkeit)

- Backup- und Recovery-Konzept
- Test der Datenwiederherstellung aus Backups
- Aufbewahrung der Datensicherung an einem sicheren Ort
- Einsatz dem Stand der Technik entsprechender Anti-Viren-Software
- Einsatz dem Stand der Technik entsprechender Software-Firewall
- Tägliche Sicherheitskopien der Daten
- Regelmäßige Anwendung von Sicherheits-Patches

8. Maßnahmen im Rechenzentrum (erbracht durch den Hosting-Dienstleister)

Die folgenden Maßnahmen werden von dem in der Subunternehmerliste aufgeführten Hosting-Dienstleister in dessen Rechenzentren erbracht und sind in dessen Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO nachgewiesen:

- Zutritt zu den Datenverarbeitungsanlagen nur nach vorheriger Anmeldung, über persönliche RFID-Karten mit zusätzlichem biometrischen Merkmal, elektrische Türöffner und Vereinzelungsanlagen
- Werkschutz rund um die Uhr sowie Alarm- und Videoanlagen an allen Ein- und Ausgängen und in den Räumlichkeiten
- Sicherheitskonzept, Alarmsystem und Rauchmelder für die Serverräume
- Zwei-Faktor-Authentifizierung für den Systemzugang und Verschlüsselung sämtlicher Datenträger
- Berechtigungskonzept nach dem Deny-Allow-Prinzip mit Protokollierung jedes Zugriffs
- Mandantenfähigkeit, Sandboxing sowie Trennung von Test- und Produktivumgebung
- Unterbrechungsfreie Stromversorgung, redundante Hardware, redundante Datenhaltung, Netztrennung und Firewalls
- Verschlüsselte Datenübertragung über Virtual Private Networks und Prüfsummen zur Erkennung unbefugter Veränderung
- Datenschutz-Management und Incident-Response-Management des Hosting-Dienstleisters

9. Sonstige Datenschutzmaßnahmen

- Regelmäßige Self-Assessments als Bestandteil eines PDCA-Zyklus
- Regelmäßige Auditierung; das Datenschutzniveau wird mindestens einmal jährlich unter Hinzuziehung externer Beratung überprüft
- Trennung von Produktiv- und Testsystem
- Nachweislich logische Trennung der Daten der jeweiligen Kunden des (Unter-)Auftragnehmers
- Eingerichtetes Datenschutz-Management
- Incident-Response-Management
- Datenschutzeinstellungen / Privacy by default

10. Überprüfung, Evaluierung und Anpassung

Der Auftragsverarbeiter wird die in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen prüfen, evaluieren und bei Bedarf anpassen.

Anlage 2 - Liste der eingesetzten Subunternehmer

Die jeweils aktuelle und abschließende Liste der eingesetzten Subunternehmer ist unter <https://lagerimgriff.de/subunternehmer/> veröffentlicht. Änderungen werden dem Auftraggeber nach Maßgabe von Ziff. 8.1 und 8.2 angezeigt.

Stand: August 2026

Frühere Fassungen dieser Allgemeinen Geschäftsbedingungen sind im AGB-Archiv abrufbar.