Auftragsverarbeitungsvertrag

gemäß Artikel 28 DSGVO

zwischen (der)

DIMEDIAL
Mindener Str. 52
32049 Herford
DEUTSCHLAND
K0951084626
- Verantwortlicher im Sinne der DSGVO, im Folgenden Auftraggeber -

und der

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Deutschland
- Auftragsverarbeiter im Sinne der DSGVO, im Folgenden Auftragnehmer -

Version	Datum	Anmerkungen
1.0	25.05.2018	Erstellung AV-Vertrag
1.1	10.02.2025	Formale und sprachliche Anpassungen
1.2	16.02.2026	Erweiterung TOMs

Einleitung

Dieser Auftragsverarbeitungsvertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den mit dem Hauptvertrag in Verbindung stehenden Verarbeitungstätigkeiten ergeben. Der AV-Vertrag gilt für alle Tätigkeiten, die die im Rahmen des Hauptvertrags erfolgen und bei denen Beschäftigte des Auftragnehmers oder von ihm beauftragte Dritte personenbezogene Daten im Auftrag des Auftraggebers verarbeiten.

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrages bestimmt sich nach dem zwischen dem Auftraggeber und dem Auftragnehmer abgeschlossenen Hauptvertrag. Der Hauptvertrag besteht aus der jeweiligen Produktbeschreibung und unseren AGB.

(2) Der Auftragnehmer verarbeitet dabei personenbezogene Daten im Sinne von Art. 4 Nr. 2 DSGVO im Auftrag des Auftraggebers.

(3) Dem Auftraggeber obliegt im Rahmen dieses Vertrages die alleinige Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften. Insbesondere stellt er sicher, dass sowohl die Übermittlung der Daten an den Auftragnehmer als auch deren Verarbeitung rechtmäßig erfolgen. Der Auftraggeber gilt als „Verantwortlicher" im Sinne des Art. 4 Abs. 7 DSGVO.

(4) Diese Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses gemäß Absatz 1 (Dauer der Auftragsverarbeitung). Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses beendet gleichzeitig diese Vereinbarung.
Das Recht zur außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

§ 2 Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten sowie Art der Daten und Kreis der Betroffenen

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen werden dem Auftragnehmer durch den Auftraggeber gemäß der vom Auftraggeber ausgefüllten Anlage 1 beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in § 1 beschriebenen Vertragsverhältnisse ergibt.

§ 3 Drittlandsübermittlung

(1) 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.

(2) 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.

(3) Der Auftragnehmer teilt dem Auftraggeber vorab mit, um welche(n) Drittstaat(en) es sich handelt und auf welche Weise das angemessene Schutzniveau im Sinne von Art. 44 ff. DSGVO für die Verarbeitung dort sichergestellt ist. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anfrage Nachweise über die implementierten Garantien zur Verfügung zu stellen.

(4) Das angemessene Schutzniveau für die Verarbeitung im Drittland wird durch eine der folgenden Maßnahmen eingehalten:

- Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO),
- verbindliche interne Datenschutzvorschriften gegebenenfalls inklusive zusätzlicher Schutzmaßnahmen (Art. 46 Abs. 2 lit. b i. V. m. 47 DSGVO),
- entsprechend modulierte Standarddatenschutzklauseln gegebenenfalls inklusive zusätzlicher Schutzmaßnahmen (Art. 46 Abs. 2 lit. c und d DSGVO),
- genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i. V. m. 40 DSGVO),
- genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i. V. m. 42 DSGVO),
- auf andere in Art. 44 ff. DSGVO vorgesehene Art und Weise, über die der Auftragnehmer den Auftraggeber vorab informiert.

§ 4 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer implementiert technische und organisatorische Maßnahmen, die einen angemessenen Schutz der Daten des Auftraggebers gewährleisten und den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) entsprechen. Dabei berücksichtigt der Auftragnehmer insbesondere das Risiko für die Rechte und Freiheiten der betroffenen Personen und stellt durch geeignete Maßnahmen sicher, dass Vertraulichkeit, Integrität, Verfügbarkeit sowie die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung dauerhaft gewährleistet sind.

(2) 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 in Anlage 2 festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind vom Auftragnehmer zu dokumentieren.

(3) Der Auftragnehmer 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.

(4) Die Dokumentation der getroffenen technischen und organisatorischen Maßnahmen findet sich in Anlage 2. Die jeweils aktuellste Version der

technischen und organisatorischen Maßnahmen kann auf der folgenden Website eingesehen werden: https://www.hetzner.com/de/AV/TOM.pdf.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Bestellung eines Datenschutzbeauftragten

Es ist ein Datenschutzbeauftragter bestellt. Dieser ist per Mail über data-protection@hetzner.com oder telefonisch unter +49 9831 505-216 zu erreichen. Weitere Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt: https://www.hetzner.com/de/unternehmen/zertifizierung/.

2. Wahrung der Vertraulichkeit

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. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung des Auftrags fort.

3. Umsetzung technischer und organisatorischer Maßnahmen

Der Auftragnehmer gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen, siehe auch § 4.

4. Zusammenarbeit mit Aufsichtsbehörden

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

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie diesen Auftrag betreffen. Dies gilt nicht für den Fall, dass die zur Offenbarung verpflichtete Partei durch gesetzliche Regelungen und/ oder behördliche oder gerichtliche Anordnung zur Verschwiegenheit über die Offenbarung verpflichtet wird. Dies gilt weiterhin nicht, soweit die zur Offenbarung verpflichtete Partei durch behördlichen oder gerichtlichen Hinweis unter Strafandrohung zur Verschwiegenheit angehalten wird.

5. Unterstützung bei behördlichen Verfahren

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. Regelmäßige Kontrolle der Maßnahmen
Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die Wirksamkeit der 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.
7. Unterstützung bei Betroffenenanfragen
Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Erfüllung von Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und das Ersuchen unverzüglich an den Auftraggeber weiterleiten.
8. Meldung von Datenschutzverletzungen
Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Die Meldung umfasst mindestens:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

§ 6 Pflichten des Auftraggebers

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten feststellt.

§ 7 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 Auftragnehmer z. B. in Form von Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der im Vertrag vereinbarten Verarbeitung personenbezogener Daten beauftragt. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen und entsprechende Vereinbarungen zu treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Der Auftraggeber stimmt der Beauftragung weiterer Subunternehmer durch den Auftragnehmer zu. Der Auftragnehmer verpflichtet sich, den Auftraggeber vor der Hinzuziehung oder der Ersetzung eines Subunternehmers rechtzeitig und in geeigneter Weise zu informieren.
Der Auftraggeber hat das Recht, einer solchen Änderung innerhalb einer angemessenen Frist von 14 Tagen aus wichtigem datenschutzrechtlichem Grund gegenüber der dem Auftragnehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Zustimmung zur Änderung als erteilt. Besteht ein wichtiger datenschutzrechtlicher Grund und kann zwischen den Parteien keine einvernehmliche Lösung gefunden werden, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(4) Die Frist von 14 Tagen verkürzt sich auf eine angemessene Frist, sofern außergewöhnliche Umstände eintreten, die ein zweiwöchiges Zuwarten für den Auftragnehmer unzumutbar machen.

(5) Die in Anlage 3 zu diesem Vertrag aufgeführten Subunternehmer gelten als genehmigt.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln überzeugen kann. Hierzu verpflichtet sich der Auftragnehmer, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(2) Der Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten kann wahlweise erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO,
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO,
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701).

(3) Der Auftragnehmer lässt die technischen und organisatorischen Maßnahmen (TOMs) in regelmäßigen Abständen, mindestens einmal jährlich, durch eine unabhängige, fachlich qualifizierte Stelle überprüfen, um die Einhaltung der datenschutzrechtlichen Anforderungen gemäß Art. 28 Abs. 3 Satz 2 lit. h DSGVO zu gewährleisten. Die Ergebnisse dieser Prüfung werden dem Auftraggeber unaufgefordert und kostenfrei unter https://accounts.hetzner.com/account/dpa zur Verfügung gestellt.

(4) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer weitere Überprüfungen gemäß Art. 28 Abs. 3 Satz 2 lit. h DSGVO zur Einhaltung der Vorschriften zum Datenschutz sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang durchzuführen. Der Auftragnehmer verpflichtet sich, den Auftraggeber bei seinen Prüfungen zur Einhaltung der Vorschriften zum Datenschutz sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu unterstützen.
Diese Prüfungen können durch den Auftraggeber selbst oder durch einen von ihm beauftragten Dritten durchgeführt werden. Sollte der vom Auftraggeber beauftragte Dritter in einem unmittelbaren Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
Der Auftraggeber ist verpflichtet, beauftragte Dritte zur Verschwiegenheit zu verpflichten. Der Auftragnehmer hat das Recht zusätzlich die Abgabe einer separaten Verschwiegenheitserklärung durch den beauftragten Dritten zu verlangen, insbesondere im Hinblick auf berufsrechtliche oder gesetzliche Verschwiegenheitspflichten.
Inspektionen vor Ort nimmt der Auftraggeber mit angemessener Vorankündigung während der üblichen Geschäftszeiten vor. Die Prüfungen müssen ohne Störung des Betriebsablaufs sowie unter Wahrung der Sicherheits- und Vertraulichkeitsinteressen des Auftragnehmers durchgeführt werden und sind auf eine Prüfung pro Kalenderjahr beschränkt. Ausgenommen hiervon sind anlassbezogene Kontrollen. Die Kosten richten sich nach § 12.

§ 9 Weitere Unterstützungspflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten. Hierzu gehören u.a.:

a. Verpflichtung zur Implementierung geeigneter technischer und organisatorischer Maßnahmen
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. Meldung von Datenschutzverletzungen gegenüber dem Auftraggeber
Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.

c. Unterstützung des Auftraggebers bezüglich seiner Informationspflicht gegenüber Betroffenen
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. Unterstützung bei Datenschutzfolgenabschätzungen
Die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

e. Unterstützung des Auftraggebers bei vorherigen Konsultationen mit der Aufsichtsbehörde
Die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten sind, über die gesetzlichen Pflichten des Auftragnehmers hinausgehen oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen. Die Höhe der Kosten orientiert sich an § 12.

§ 10 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer und jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen die Daten, die Gegenstand dieses Vertrages sind, ausschließlich im Rahmen des Auftrags und gemäß den Weisungen des Auftraggebers verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind oder ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a DSGVO vorliegt und dessen Voraussetzungen gewahrt werden.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können anschließend vom Auftraggeber schriftlich oder in Textform (z. B. E-Mail) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens Textform). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen die DSGVO oder andere Datenschutzbestimmungen der EU oder des Mitgliedstaates [Remonstrationspflicht]. 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

(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) Daten, Datenträger sowie sämtliche Dokumente sind nach Auftragsende auf Verlangen (schriftlich oder in Textform) des Auftraggebers entweder herauszugeben, sofern sie im Eigentum des Auftraggebers sind, oder zu löschen.

(3) Sofern eine datenschutzkonforme Löschung dieser Daten nicht möglich ist, stellt der Auftragnehmer eine datenschutzkonforme Vernichtung der Datenträger und Unterlagen, die vertragsgegenständliche Daten enthalten, sicher.
Sollten aufgrund abweichender Vorgaben bei der Herausgabe oder Löschung der Daten zusätzliche Kosten entstehen, so trägt diese Kosten der Auftraggeber. Die Kosten orientieren sich an § 12 des Vertrages.

(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Der Auftragnehmer kann diese Dokumentation zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 12 Entgelte

(1) Die Höhe des vorab zu vereinbarenden Entgelts für die in §§ 8, 9 und 11 genannten Rechte orientiert sich an einem festzulegenden Stundensatz des vom Auftragnehmer für die Betreuung abgestellten Mitarbeiters.

(2) Der Vergütungsanspruch seitens des Auftragnehmers besteht nicht bei Leistungen, welche aufgrund von Verstößen gegen Datenschutzgesetze des Auftragnehmers erforderlich sind.

§ 13 Sonstige

13.1 Rechtswahl

Es gilt das Recht der Bundesrepublik Deutschland.
Ausschließlicher, auch internationaler Gerichtsstand für alle sich aus dem Vertragsverhältnis ergebenden Streitigkeiten ist unser Geschäftssitz in Gunzenhausen. Wir sind jedoch in allen Fällen berechtigt, am Sitz des Kunden zu klagen. Vorrangige gesetzliche Vorschriften, insbesondere zu ausschließlichen Zuständigkeiten, bleiben unberührt.

13.2 Haftungsregelung

Eine zwischen den Parteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung.

13.3 Verwahrung der Daten

Sollten die Daten des Auftraggebers beim Auftragnehmer aufgrund von Pfändung, Beschlagnahme, einem Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
Dies gilt nicht für den Fall, dass die zur Offenbarung verpflichtete Partei durch gesetzliche Regelungen und/oder behördliche oder gerichtliche Anordnung zur Verschwiegenheit über die Offenbarung verpflichtet wird. Dies gilt weiterhin nicht, soweit die zur Offenbarung verpflichtete Partei durch behördlichen oder gerichtlichen Hinweis unter Strafandrohung zur Verschwiegenheit angehalten wird.

13.4 Änderungen und Ergänzungen

Änderungen und Ergänzungen dieses Vertrages sowie dessen Bestandteile, einschließlich etwaiger Zusicherungen des Auftragnehmers, bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann. Dabei ist ausdrücklich kenntlich zu machen, dass es sich um eine Änderung oder Ergänzung dieser Bedingungen handelt. Gleiches gilt für den Verzicht auf dieses Formerfordernis.

13.5 Vorrang von Datenschutzregelungen

Bei etwaigen Widersprüchen gehen Regelungen dieses AV-Vertrages zum Datenschutz den Regelungen des Hauptvertrages vor.

13.6 Salvatorische Klausel

Sollten einzelne Teile dieses Vertrages unwirksam sein, bleibt die Gültigkeit der übrigen Regelungen davon unberührt.

Unterschriften

_____, den _____

Auftraggeber

Gunzenhausen, den 04.09.2026



Auftragnehmer

Anlage 1: Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten sowie Art der Daten und der Kreis der Betroffenen

Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Ergeben sich direkt aus dem Hauptvertrag.

Art der Daten

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten
- Protokolldaten
- Vertragsabrechnungs- und Zahlungsdaten

Kreis der Betroffenen

- Kunden und Interessenten des Auftraggebers
- Mitarbeiter und Lieferanten des Auftraggebers

Anlage 2: Technische und organisatorische Maßnahmen (TOMs) nach Artikel 32 DSGVO

Die technischen und organisatorischen Maßnahmen (TOMs) dienen dazu, ein angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten und insbesondere die Rechte und Freiheiten betroffener Personen zu schützen. Im Folgenden stellen wir die von uns implementierten TOMs vor.

Detailliertere Informationen zu einzelnen Maßnahmen finden Sie unter: https://docs.hetzner.com/de/general/others/technical-and-organizational-measures.

1 Zutrittskontrolle

Die Zutrittskontrolle regelt, wer physischen Zugang zu einem Gelände, Gebäude oder Raum erhält.

Maßnahme	Rechenzentrumsstandorte	Verwaltungsgebäude
Elektronisches Zutrittskontrollsystem mit Protokollierung	✓	✓
Dokumentierte Vergabe von Zutrittsmedien	✓	✓
Flächendeckende Videoüberwachung	✓	✓
Richtlinie zum Besuchermanagement	✓	✓
Hochsicherheitszaun mit Übersteig- und Untergrabenschutz um den gesamten Datacenter-Park	✓	Nicht zutreffend
Separierte Colocation-Bereiche mit abschließbaren Racks	✓	Nicht zutreffend

Bitte beachten Sie für die nachstehenden Kapitel den folgenden Hinweis:
Bei unseren dedizierten Servern / Cloud Servern liegt die Verantwortung für die Verwaltung, Wartung und Sicherheit der Serverinfrastruktur vollständig beim Auftraggeber.
Bei unseren Managed-Produkten übernehmen wir die Verantwortung für die Wartung, Administration und Sicherheit Ihrer Systeme.

2 Zugangskontrolle

Die Zugangskontrolle definiert, wer sich auf einem System einloggen darf, sodass nur autorisierte Personen Zugriff auf dieses erhalten.

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Eigenes Kundenkonto mit zahlreichen Verwaltungsoptionen und Zugang zur Administrationsoberfläche	✓	✓	✓	✓	✓	✓	✓	✓
Nachvollziehbare Protokollierung von Zugriffs- und Änderungsvorgängen im Kundenaccount	✓	✓	✓	✓	✓	✓	✓	✓
Passwortpflicht für das Kundenkonto mit festgelegten Mindestanforderungen	✓	✓	✓	✓	✓	✓	✓	✓
Option zur Zwei-Faktor-Authentifizierung (2FA) für Kundenkonto	✓	✓	✓	✓	✓	✓	✓	✓
Serverzugriff erfolgt ausschließlich durch Auftraggeber	✓	✓	✓	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Administrativer Zugriff erfolgt ausschließlich durch autorisierte Hetzner-Mitarbeitende im Rahmen der vereinbarten Leistung über mehrstufige Authentifizierung und kryptografischem Schutz (je nach Produkt von reiner Infrastrukturwartung bis hin zu vollständiger Serververwaltung)	Nicht zutreffend (siehe vorherige Zeile)	Nicht zutreffend (siehe vorherige Zeile)	Nicht zutreffend (siehe vorherige Zeile)	✓	✓	✓	✓	✓
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓	✓	✓	✓	✓	✓

3 Zugriffskontrolle

Die Zugriffskontrolle regelt, welche Berechtigungen eine Person innerhalb eines Systems hat. Sie bestimmt, was ein Benutzer nach erfolgreichem Zugang sehen, ändern oder ausführen darf.

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Regelmäßige Sicherheitsupdates	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓ für zugrunde liegende Cloud-Infrastruktur	✓ für zugrunde liegende Infrastruktur	✓	✓	✓	✓
Revisionssicheres, verbindliches Berechtigungsverfahren auf Basis eines Rollen- und Berechtigungskonzeptes	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓ Für Zugriffe auf die Cloud-Infrastruktur. Für virtuellen Server ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich	✓ Für Dateizugriffe ist Auftraggeber selbst verantwortlich
Pflege, Sicherheit und Aktualität der übertragenen Daten/Software	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓ bzgl. Zugriffe auf Cloud-Server	✓	✓	✓	✓	✓

4 Datenträgerkontrolle

Die Datenträgerkontrolle umfasst Maßnahmen und Verfahren, die sicherstellen, dass die Nutzung, der Zugriff und der Transport von physischen Datenträgern kontrolliert und vor unbefugtem Zugriff geschützt werden.

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Definiertes Verfahren zur Löschung von Festplattendaten nach Auftragsbeendigung (je nach Produktart unterschiedlich umgesetzt)	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓	✓
Physische Zerstörung von Datenträgern bei nicht erfolgreicher Datenlöschung	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓	✓
Physischer Zugriff auf Datenträgern nur in definierten Bereichen; Transport standortübergreifend ausschließlich in verschlossenen Transportboxen.	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓	✓

5 Trennungskontrolle

Maßnahmen zur Trennungskontrolle stellen sicher, dass Daten unterschiedlicher Kunden oder Anwendungen innerhalb eines Systems klar voneinander getrennt verarbeitet und gespeichert werden.

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Physische oder logische Trennung von Daten	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓	✓
Physische und logische Trennung von Backup-Daten	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	Nicht zutreffend	Obliegt Auftrag-geber
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓	✓	✓	✓	Nicht zutreffend	Nicht zutreffend

6 Pseudonymisierung

Durch Maßnahmen zur Pseudonymisierung werden personenbezogene Daten so modifiziert, dass sie nur unter Verwendung von Zusatzinformationen einer bestimmten Person zugeordnet werden können.

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Pseudonymisierung der auf den Systemen gespeicherten Daten	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber

7 Vertraulichkeit

Maßnahmen zur Vertraulichkeit stellen sicher, dass personenbezogene Daten bei der Verarbeitung und Speicherung vor unberechtigtem Zugriff oder Weitergabe geschützt werden.

Maßnahme	Allgemein
Verpflichtungserklärung der Hetzner-Mitarbeitenden vor Tätigkeitsbeginn zur datenschutzkonformen Verarbeitung personenbezogener Daten	✓
Verpflichtungserklärung externer Personen vor Tätigkeitsbeginn zu Verschwiegenheit und Umsetzung von TOMs (bei Bedarf)	✓
Regelmäßige Sensibilisierungen und Schulungen der Hetzner-Mitarbeitenden bzgl. Datenschutz- und Informationssicherheitsthemen	✓
Verschlüsselungsoptionen für die Datenübertragung (je nach Produktart unterschiedlich umgesetzt)	✓
Verschlüsselung der Daten (at rest)	Obliegt Auftraggeber
Verschlüsselung des Backups (at rest)	Obliegt Auftraggeber. Ausnahme Managed-Server: ✓

8 Integrität

Die Integrität stellt sicher, dass Daten und Systeme vollständig, unverfälscht und korrekt bleiben – sowohl bei der Speicherung als auch bei der Übertragung.

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Protokollierung von Datenänderungen	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓
Verantwortung für Eingabe und Bearbeitung von Daten	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber
Virenscanner / Sicherheitsprüfung	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	Rootkit-Prüfungen	Rootkit-Prüfungen	-
Zusätzliche Maßnahmen obliegen Auftraggeber	✓	✓	✓	✓	✓	✓	✓	✓

9 Verfügbarkeit, Belastbarkeit und Netzwerksicherheit

Die Verfügbarkeit fokussiert sich auf die kontinuierliche Funktionsfähigkeit eines Systems. Die Belastbarkeit sorgt in diesem Zusammenhang dafür, dass die Verfügbarkeit auch unter außergewöhnlichen Umständen gewährleistet bleibt. Die Netzwerksicherheit umfasst Maßnahmen zum Schutz der Netzwerkinfrastruktur von unbefugten Zugriffen und Angriffen.

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Betrieb & Support								
24/7 technischer Support direkt im Rechenzentrum	Nicht zutreffend Remote Hands auf Anfrage	✓	✓	✓	✓	✓	✓	✓
Eskalationskette für Störungen und Notfälle	siehe Produktbeschreibung							
Monitoring	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓ für Host Für virtuellen Server ist Auftraggeber selbst verantwortlich	✓	✓	✓	✓	✓
Stromversorgung, Klimatisierung und Gebäudetechnik								
Unterbrechungsfreie Stromversorgung durch redundante USVs und NEA	✓	✓	✓	✓	✓	✓	✓	✓
Redundanten Stromeinspeisung vom Umspannwerk	✓	✓	✓	✓	✓	✓	✓	✓

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Redundante und energieeffiziente Kühlung durch direkte freie Kühlung und Klimaanlagen	✓	✓	✓	✓	✓	✓	✓	✓
Kaltgangeinhausung in überdurchschnittlich hohem Doppelboden	✓	✓	✓	✓	✓	✓	✓	✓
Überwachung der prozessrelevanten Größen über intelligentes Mess-, Steuer-, Regel- und Überwachungssystem	✓	✓	✓	✓	✓	✓	✓	✓
Brandschutz								
Flächendeckende Brandfrüherkennungsmechanismen mit automatischer Alarmierung und Leitstellenanbindung	✓	✓	✓	✓	✓	✓	✓	✓
Dynamisches Brandschutzkonzept	✓	✓	✓	✓	✓	✓	✓	✓
Regelmäßige Schulungen und Notfallübungen der Brandschutzhelfer	✓	✓	✓	✓	✓	✓	✓	✓

Maßnahme	Colo-cation	Dedicated Server	Cloud Server	Managed Server	Web-hosting	Storage Share	Storage Box	Object Storage
Netzwerk & Angriffsschutz								
Redundante und hochverfügbare Netzwerkinfrastruktur (99,9%ige Netzwerkverfügbarkeit gemäß AGB)	✓	✓	✓	✓	✓	✓	✓	✓
Dauerhaft aktive DDoS-Erkennung	✓	✓	✓	✓	✓	✓	✓	✓
Einsatz von Firewall und Portreglementierungen	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓
Individuell konfigurierbare Firewall	Nicht zutreffend	✓	✓	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	Nicht zutreffend (siehe nächste Zeile)	✓
Providerverwaltete Firewall mit 24/7-Monitoring	Nicht zutreffend	Nicht zutreffend (siehe vorherige Zeile)	Nicht zutreffend (siehe vorherige Zeile)	✓	✓	✓	✓	Nicht zutreffend (siehe vorherige Zeile)
Backup & Systemschutz								
Backup- und Recovery-Konzept	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber Backup/Snapshots können kostenpflichtig hinzugebucht werden	✓ zum Teil abhängig von gebuchten Leistungen	✓	✓ eigenes Backup empfohlen	Obliegt Auftrag-geber Snapshots, abhängig von gebuchter Leistung	Obliegt Auftrag-geber Redundante Speicherung innerhalb des Clustersystems
Festplattenspieglung	Obliegt Auftrag-geber	Obliegt Auftrag-geber	Obliegt Auftrag-geber	✓	✓	✓	✓	✓

10 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Regelmäßige Überprüfungs-, Bewertungs- und Evaluierungsverfahren gewährleisten die kontinuierliche Einhaltung und Verbesserung von Datenschutz- und Sicherheitsstandards.

Maßnahme	Allgemein
Datenschutz-Informationssicherheits-Management-System (DMS, ISMS)	✓
Bestellung eines Datenschutz- und Informationssicherheitsbeauftragten und Einbindung dieser in betriebliche Prozesse	✓
Datenschutzfreundliche Voreinstellungen bei Softwareentwicklungen (Privacy by default und Privacy by design)	✓
Incident-Response-Management	✓
Zertifizierung nach ISO 27001, § 8a BSI-KritisV und BSI C5 Typ 2 Testat	✓
Jährliche Überprüfung der TOMs durch externen Dienstleister	✓
Jährliche Überprüfung der ordnungsgemäßen Verbindungspreisberechnung über Sachverständigengutachten gemäß § 63 TKG	✓
EMAS-Zertifizierung (ISO 14001) des Umweltmanagementsystems der deutschen Standorte	✓

Anlage 3: Genehmigte Subunternehmer

Die Hetzner Online GmbH (Auftragnehmer) nimmt für die Datenverarbeitung im Auftrag des Hetzner-Kunden (Auftraggeber) Leistungen von Dritten in Anspruch, die im Auftrag der Hetzner Online GmbH Daten verarbeiten (Subunternehmer).
Die folgenden Unternehmen sind als Subunternehmer genehmigt:

Serverstandort	Name des Subunternehmens	Anschrift des Subunternehmens	Art der Leistung
Finnland	Hetzner Finland Oy	Huurrekuja 10, 04360 Tuusula (Finnland)	Gebäudevermietung, Technischer Support
USA	Hetzner US LLC	1500 Broadway, 19th Fl, New York, NY 10036 (USA)	Vermietung von Servern am Standort USA
	NTT Global Data Centers Americas, Inc.	1 625 National Drive, Sacramento, CA 95834 (USA)	Colocation-Anbieter am Standort USA
	QTS Investment Properties Hillsboro, LLC	Overland Park, 12851 Foster Street, Overland Park, KS 66213 (USA)	Colocation-Anbieter am Standort USA
Singapur	Hetzner Singapore Pte. Ltd.	1 Scotts Road, #21-10 Shaw Centre, Singapore 228208 (Singapur)	Vermietung von Servern am Standort Singapur
	NTT Global Data Centers SG1 Pte Ltd	8 Kallang Avenue #15-01/09, Aperia, 339509 Singapore (Singapur)	Colocation-Anbieter am Standort Singapur

Bitte beachten Sie den folgenden Hinweis:
Soweit Sie sich für einen Serverstandort in der EU entschieden haben, werden Ihre Serverdaten ausschließlich innerhalb der EU verarbeitet. Supportdienstleistungen erfolgen für alle Serverstandorte innerhalb der EU.