Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Fassung 4.1 vom 09.10.2026

nach Art. 28 DSGVO

zwischen

dem Auftraggeber, der ein Angebot des Auftragnehmers annimmt, das auf diesen Vertrag verweist, – nachfolgend „Auftraggeber" oder „Verantwortlicher" –

und

Daniel Jacobs, IT-Service Zedernstraße 5, 48531 Nordhorn info@itservice-danieljacobs.de · 0172 3096988 – nachfolgend „Auftragnehmer" oder „Auftragsverarbeiter" –

Vorbemerkung

Der Auftragnehmer erbringt für den Auftraggeber IT-Leistungen, bei denen er auf personenbezogene Daten zugreift, die der Auftraggeber verantwortet. Je nach Leistung arbeitet er dabei in Systemen des Auftraggebers oder betreibt Websites und Anwendungen auf eigener Infrastruktur.

Dieser Vertrag ist ein **einheitlicher Vertrag für alle Auftraggeber**. Was im Einzelfall beauftragt ist, ergibt sich aus dem **Angebot** (Hauptvertrag) und den dort genannten **Leistungsbausteinen** nach Anlage 1.

Der Auftraggeber bleibt Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO; er entscheidet allein über Zweck und Mittel der Verarbeitung. Dieser Vertrag regelt die Verarbeitung im Auftrag nach Art. 28 DSGVO. Er gilt zusätzlich zum Hauptvertrag; bei Widersprüchen in Datenschutzfragen geht dieser Vertrag vor.

---

§ 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

1.1 Gegenstand. Gegenstand ist die Erbringung der im Hauptvertrag vereinbarten Leistungen. Welche **Leistungsbausteine** nach Anlage 1 beauftragt sind, steht im Angebot. Für jeden beauftragten Baustein gelten die dort beschriebenen Angaben zu Art der Verarbeitung, betroffenen Personen und Datenarten.

1.2 Art der Verarbeitung. Erheben, Erfassen, Auslesen, Abfragen, Ordnen, Speichern, Anpassen, Verändern, Verwenden, Übermitteln, Löschen und Vernichten — jeweils nur, soweit der beauftragte Baustein es erfordert.

1.3 Zweck. Ausschließlich die Erbringung der beauftragten Leistung. Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt. Insbesondere werden die Daten nicht ausgewertet, nicht mit anderen Beständen zusammengeführt und nicht zum Training von KI-Modellen verwendet.

1.4 Betroffene Personen und Datenarten ergeben sich aus Anlage 1 für den jeweiligen Baustein.

1.5 Was nur mit Zusatzvereinbarung verarbeitet wird. Die folgenden Verarbeitungen sind von diesem Vertrag **nicht** gedeckt, solange die Parteien keine gesonderte Zusatzvereinbarung in Textform geschlossen haben:

a) Daten besonderer Kategorien nach Art. 9 DSGVO (etwa Gesundheitsdaten), b) Daten über strafrechtliche Verurteilungen nach Art. 10 DSGVO, c) Beschäftigtendaten, die über Namen, dienstliche Kontaktdaten und Zugangsdaten für die betriebenen Anwendungen hinausgehen, d) Tätigkeiten für Auftraggeber, die einer Schweigepflicht nach § 203 StGB unterliegen (§ 1.8).

Der Auftraggeber teilt dem Auftragnehmer vor Beginn mit, wenn einer dieser Fälle vorliegt (§ 8.2). Bis zum Abschluss der Zusatzvereinbarung nimmt der Auftragnehmer die betreffende Verarbeitung nicht auf.

1.6 Dauer. Der Vertrag beginnt mit seinem Abschluss nach § 11 und endet mit dem Ende des Hauptvertrags. Die Pflichten aus § 7 und § 9 gelten darüber hinaus fort.

1.7 Ort der Verarbeitung. Die Verarbeitung findet in Deutschland statt. Sicherungen und Leistungen von Unterauftragsverarbeitern werden an den in Anlage 3 genannten Orten erbracht. Eine Verarbeitung in einem Drittland findet nur statt, soweit sie sich aus dem Einsatz eines in Anlage 3 genannten Unterauftragsverarbeiters ergibt und die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

1.8 Berufsgeheimnis. Unterliegt der Auftraggeber einer beruflichen Schweigepflicht nach § 203 StGB — insbesondere als Angehöriger eines Heilberufs, als Rechtsanwalt, Steuerberater oder Angehöriger einer vergleichbaren Berufsgruppe —, weist er den Auftragnehmer darauf vor Beginn der Verarbeitung hin. Der Auftragnehmer ist in diesem Fall „sonstige mitwirkende Person" im Sinne des § 203 Abs. 3 StGB und wird **gesondert schriftlich zur Geheimhaltung verpflichtet**. Diese Verpflichtung ist nicht Gegenstand dieses Vertrags, sondern wird in einem eigenen Dokument erklärt; sie ist **vor dem ersten Zugriff** zu erteilen. Ohne sie nimmt der Auftragnehmer die Tätigkeit nicht auf.

§ 2 Weisungsrecht des Auftraggebers

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Der Hauptvertrag und dieser Vertrag stellen die Erstweisung dar.

2.2 Weisungen ergehen in Textform; E-Mail genügt. Weisungsberechtigt ist die im Angebot genannte Ansprechperson des Auftraggebers sowie, wer vom Auftraggeber in Textform als weisungsberechtigt benannt wird. Mündlich erteilte Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

2.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Er ist berechtigt, die Ausführung einer solchen Weisung auszusetzen, bis der Auftraggeber sie bestätigt oder ändert.

2.4 Ist der Auftragnehmer nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet, teilt er dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

2.5 Maßnahmen im laufenden Betrieb. Bei Baustein 3 sind Handlungen, die der Aufrechterhaltung des sicheren Betriebs dienen — Einspielen von Sicherheitsaktualisierungen, Sperren auffälliger Zugriffe, Neustart von Diensten, Wiederherstellung nach einer Störung —, von der Erstweisung gedeckt und bedürfen keiner Einzelweisung. Eingriffe, die über den Regelbetrieb hinausgehen, hält der Auftragnehmer fest.

§ 3 Pflichten des Auftragnehmers

3.1 Vertraulichkeit. Der Auftragnehmer führt das Gewerbe als Einzelunternehmen ohne Beschäftigte. Er ist selbst zur Vertraulichkeit verpflichtet. Setzt er künftig Personen ein, verpflichtet er diese vor Aufnahme der Tätigkeit schriftlich zur Vertraulichkeit und weist sie auf die einschlägigen Datenschutzvorschriften hin (Art. 28 Abs. 3 lit. b DSGVO).

3.2 Datensicherheit. Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Diese sind in Anlage 2 beschrieben. Er darf sie fortentwickeln, sofern das Schutzniveau nicht unterschritten wird.

3.3 Zugangsmodelle. Für den Zugang zu Konten und Systemen gilt eines der folgenden Modelle; sie können nebeneinander gelten, etwa Modell C für den Server und Modell A für das E-Mail-Postfach des Auftraggebers:

- **Modell A — eigene Berechtigung.** Der Auftraggeber ist Inhaber seiner Konten bei den beteiligten Anbietern und erteilt dem Auftragnehmer eine eigene, personengebundene Berechtigung. Zugangsdaten werden nicht weitergegeben.
- **Modell B — treuhänderische Verwaltung.** Die Konten laufen auf den Namen des Auftraggebers, werden aber vom Auftragnehmer eingerichtet und verwaltet, oder der Auftragnehmer hält Zugangsdaten des Auftraggebers dauerhaft. Es gilt zusätzlich § 3.4.
- **Modell C — Betrieb auf Infrastruktur des Auftragnehmers.** Server und Vertrag mit dem Rechenzentrumsbetreiber laufen auf den Auftragnehmer. Gilt immer bei Baustein 3. Es gelten zusätzlich § 3.10 und § 3.11.

Ohne abweichende Angabe im Angebot gilt **Modell C für Baustein 3 und Modell A für alles Übrige**. Ergibt sich während der Zusammenarbeit, dass der Auftragnehmer Zugangsdaten des Auftraggebers dauerhaft halten muss, gilt dafür Modell B; der Auftragnehmer teilt dies dem Auftraggeber in Textform mit.

3.4 Pflichten bei treuhänderischer Verwaltung (Modell B). Der Auftragnehmer

a) bewahrt Zugangsdaten des Auftraggebers ausschließlich in einem verschlüsselten Passwortmanager auf — niemals in Tabellen, Notizen oder E-Mails. Davon ausgenommen sind **Dienstzugangsdaten, die der laufende Betrieb dauerhaft benötigt** — etwa das Kennwort des Postfachs, über das eine Website ihre Nachrichten versendet, oder ein Schnittstellenschlüssel. Diese liegen zusätzlich im Geheimnisspeicher des Bausystems und in einer Konfigurationsdatei auf dem Server, die außerhalb des ausgelieferten Verzeichnisses liegt, nur dem Dienst selbst lesbar ist und über keine Internetadresse abrufbar ist. Sie werden nicht in die Versionsverwaltung aufgenommen und nicht in Protokollen ausgegeben, b) sichert alle betroffenen Konten, soweit der Anbieter es zulässt, mit Zwei-Faktor-Authentifizierung ab, c) verwendet die Zugangsdaten ausschließlich zur Erfüllung des Hauptvertrags, d) übergibt dem Auftraggeber auf dessen Verlangen jederzeit, spätestens bei Vertragsende, sämtliche Zugangsdaten in einer für ihn nutzbaren Form und weist ihn dabei in Textform darauf hin, die Zugangsdaten unverzüglich zu ändern, und e) löscht die Zugangsdaten nach der Übergabe unverzüglich aus dem eigenen Bestand und bestätigt die Löschung auf Verlangen in Textform.

Der Auftraggeber bleibt in den Modellen A und B Inhaber der Konten und der zugehörigen Vertragsverhältnisse.

3.5 Zugang nur zur Einrichtung. Erhält der Auftragnehmer Zugang zu einem Konto des Auftraggebers allein, um es einzurichten, ist dieser Zugang auf die Einrichtung befristet. Nach Abschluss gibt er die Zugangsdaten zurück, weist den Auftraggeber in Textform darauf hin, das Kennwort zu ändern, und löscht sie aus dem eigenen Bestand. Bleibt ein Zugang für den laufenden Betrieb erforderlich, gilt § 3.4.

3.6 Datenschutzbeauftragter. Ein Datenschutzbeauftragter ist beim Auftragnehmer nicht zu benennen; die Voraussetzungen des § 38 BDSG liegen nicht vor. Ansprechpartner in Datenschutzfragen ist Daniel Jacobs, info@itservice-danieljacobs.de.

3.7 Trennung. Daten verschiedener Auftraggeber werden getrennt verarbeitet und gespeichert. Auf dem gemeinsam genutzten Server läuft je Auftraggeber ein eigener, gekapselter Dienst mit eigenem Datenbestand und eigenen Zugangsdaten; ein Dienst kann nicht auf den Datenbestand eines anderen zugreifen.

3.8 Datenschutz durch Technikgestaltung. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung von Art. 25 DSGVO, insbesondere durch datensparsame Voreinstellungen, Berechtigungen mit den geringstmöglichen Rechten und die Vermeidung nicht erforderlicher Datenflüsse.

3.9 Speicherorte. Personenbezogene Daten des Auftraggebers verarbeitet der Auftragnehmer

a) in den Systemen und Konten des Auftraggebers, soweit ihm dort Zugang eingeräumt ist, b) bei Baustein 3 auf dem Server und in dessen Sicherungen nach Anlage 3, c) lokal auf seinen Arbeitsgeräten, soweit für Fehlersuche und Pflege erforderlich, und d) bei den übrigen in Anlage 3 genannten Unterauftragsverarbeitern für den dort genannten Zweck.

Eine Ablage in weiteren Diensten findet nicht statt. Unterlagen ohne Personenbezug — etwa Angebote, Vertragsentwürfe, Quellcode und technische Dokumentation — sind hiervon nicht erfasst.

3.10 Betrieb, Sicherung und Wiederherstellung (Baustein 3). Der Auftragnehmer

a) hält Betriebssystem und eingesetzte Dienste auf einem gepflegten Stand und spielt sicherheitsrelevante Aktualisierungen zeitnah ein, b) erstellt **mindestens täglich** eine verschlüsselte Sicherung der betriebsrelevanten Daten und bewahrt sie **an einem vom Server getrennten Ort** auf, c) bewahrt Sicherungen **90 Tage** auf und löscht sie danach automatisch, d) überwacht den Betrieb automatisiert und wird bei Störungen benachrichtigt, e) prüft die Wiederherstellbarkeit aus einer Sicherung **mindestens einmal jährlich** und hält das Ergebnis fest, und f) gibt dem Auftraggeber auf Verlangen Auskunft über den Stand dieser Maßnahmen.

3.11 Keine Verfügbarkeitszusage. Dieser Vertrag regelt den Datenschutz. Eine bestimmte Verfügbarkeit, Reaktions- oder Wiederherstellungszeit wird durch ihn **nicht** zugesagt; solche Zusagen bedürfen einer gesonderten Vereinbarung im Hauptvertrag. Unberührt bleibt die Pflicht aus Art. 32 Abs. 1 lit. b und c DSGVO, Verfügbarkeit und Belastbarkeit der Systeme sowie die Wiederherstellbarkeit nach einem Zwischenfall auf einem dem Risiko angemessenen Niveau sicherzustellen.

§ 4 Unterauftragsverarbeiter

4.1 Allgemeine Genehmigung. Der Auftraggeber erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 3 genannten Unterauftragsverarbeiter. Für einen Auftraggeber werden nur die Unterauftragsverarbeiter tätig, deren Zeile in Anlage 3 zu einem von ihm gebuchten Baustein gehört.

4.2 Änderungen. Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, teilt er dies dem Auftraggeber **mindestens vier Wochen vorher** in Textform mit, sofern der Auftraggeber einen betroffenen Baustein gebucht hat. Zusätzlich wird die geänderte Anlage 3 unter der in § 10.3 genannten Adresse veröffentlicht. Der Auftraggeber kann innerhalb von zwei Wochen nach Zugang aus wichtigem, datenschutzbezogenem Grund widersprechen.

4.3 Widerspricht der Auftraggeber und lässt sich die Leistung ohne den betreffenden Unterauftragsverarbeiter nicht mit zumutbarem Aufwand erbringen, kann jede Partei den betroffenen Teil des Hauptvertrags mit einer Frist von einem Monat kündigen. Bereits erbrachte Leistungen sind zu vergüten.

4.4 Der Auftragnehmer schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem dieselben Datenschutzpflichten auferlegt, die ihn selbst treffen. Er bleibt dem Auftraggeber gegenüber für die Einhaltung verantwortlich.

4.5 Keine Unterauftragsverarbeitung im Sinne dieser Regelung sind Nebenleistungen wie Telekommunikation, Post, Wartung von Geräten sowie die Entsorgung von Datenträgern. Für diese stellt der Auftragnehmer die Vertraulichkeit auf andere geeignete Weise sicher.

4.6 Anbieter des Auftraggebers. Anbieter, mit denen **der Auftraggeber** selbst einen Vertrag unterhält — etwa sein Domainanbieter, sein E-Mail-Postfach, sein Shopsystem, sein Hoster oder ein eigener KI-Zugang —, sind keine Unterauftragsverarbeiter des Auftragnehmers. Das gilt auch, wenn der Auftragnehmer diese Konten nach Modell B verwaltet. Mit diesen Anbietern schließt der Auftraggeber die erforderlichen Verträge nach Art. 28 DSGVO selbst ab und prüft bei Anbietern außerhalb der EU die Voraussetzungen der Art. 44 ff. DSGVO. Der

Auftragnehmer weist ihn auf diese Pflicht hin und unterstützt ihn auf Wunsch, kann sie ihm aber nicht abnehmen.

4.7 KI-gestützte Werkzeuge. Werden personenbezogene Daten des Auftraggebers in ein KI-gestütztes Werkzeug eingegeben — auch als Beispieldatensatz, als Fehlermeldung mit echten Namen, als Bildschirmfoto oder als Auszug aus einer Protokolldatei —, ist der Anbieter dieses Werkzeugs Unterauftragsverarbeiter. Der Auftragnehmer tut dies **nur** mit Anbietern, die in Anlage 3 für diesen Zweck aufgeführt sind. Für seine eigene Arbeit — Entwicklung, Fehlersuche und Beratung — gibt er keine personenbezogenen Daten des Auftraggebers in KI-Werkzeuge ein, sondern beschreibt Struktur, Format und Fehlerbild; das schließt **unbearbeitete Protokollauszüge mit IP-Adressen** ausdrücklich ein. Quellcode, Konfigurationen und technische Dokumentation ohne Personenbezug sind hiervon nicht erfasst.

§ 5 Unterstützung des Auftraggebers

5.1 Betroffenenrechte. Wendet sich eine betroffene Person mit einem Antrag nach den Art. 15 bis 22 DSGVO an den Auftragnehmer, leitet er den Antrag unverzüglich an den Auftraggeber weiter und beantwortet ihn nicht selbst. Er unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung nachzukommen (Art. 28 Abs. 3 lit. e DSGVO). Dazu gehört auf Weisung auch die Auskunft darüber, welche Daten aus dem Betrieb zu einer Person vorliegen.

5.2 Meldepflichten. Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten aus dem Auftragsverhältnis unverzüglich, **spätestens innerhalb von 48 Stunden nach Kenntnis**. Die Meldung enthält, soweit im Zeitpunkt der Meldung bekannt: Art der Verletzung, betroffene Datenkategorien, ungefähre Zahl der Betroffenen und Datensätze, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen. Sind noch nicht alle Angaben verfügbar, meldet der Auftragnehmer zunächst mit dem verfügbaren Kenntnisstand und reicht das Übrige nach; die Meldung darf dadurch nicht verzögert werden.

5.3 Melden ist nicht Beheben. Die Meldung nach § 5.2 ist eine Informationspflicht. Sie umfasst weder eine vollständige forensische Aufklärung noch die Benachrichtigung betroffener Personen. Die Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO und die Benachrichtigung betroffener Personen nach Art. 34 DSGVO obliegen dem Auftraggeber.

Der Auftragnehmer ergreift von sich aus die Sofortmaßnahmen, die in seinem Verantwortungsbereich liegen und keinen Aufschub dulden — etwa das Sperren eines kompromittierten Zugangs, das Abschalten eines betroffenen Dienstes oder das Einspielen einer Sicherung. **Bei Baustein 3 ist die Beseitigung der Ursache im Verantwortungsbereich des Servers Teil der beauftragten Leistung** und nicht gesondert zu vergüten. Darüber hinausgehende Aufklärungs- und Wiederherstellungsleistungen, insbesondere solche im Verantwortungsbereich des Auftraggebers, sind gesondert zu beauftragen und werden nach § 5.5 vergütet.

5.4 Weitere Unterstützung. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Art. 32 bis 36 DSGVO, insbesondere bei einer Datenschutz-Folgenabschätzung und einer vorherigen Konsultation der Aufsichtsbehörde, jeweils unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

5.5 Vergütung. Unterstützungsleistungen nach § 5 und Nachweise nach § 6 erbringt der Auftragnehmer unentgeltlich, soweit sie auf einem von ihm zu vertretenden Umstand beruhen oder den üblichen Rahmen nicht überschreiten. Darüber hinausgehender Aufwand wird nach dem im Hauptvertrag vereinbarten Satz vergütet.

§ 6 Nachweise und Kontrollen

6.1 Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind.

6.2 Der Auftraggeber kann sich von der Einhaltung überzeugen. Der Nachweis kann erfolgen durch Selbstauskunft, Vorlage der aktuellen Fassung der Anlage 2, ein aussagekräftiges Testat einer unabhängigen Stelle oder ein anerkanntes Zertifikat. Für den Rechenzentrumsbetreiber legt der Auftragnehmer dessen Zertifikate und Auftragsverarbeitungsvertrag vor.

6.3 Genügt dies im Einzelfall nicht, ermöglicht der Auftragnehmer eine Überprüfung vor Ort. Sie ist mit angemessener Frist von in der Regel zwei Wochen anzukündigen, auf das erforderliche Maß zu beschränken und während der üblichen Geschäftszeiten durchzuführen. Ein Zutritt zum Rechenzentrum richtet sich nach den Bedingungen des Betreibers. Der Auftraggeber trägt seine Kosten selbst; der Aufwand des Auftragnehmers wird nach § 5.5 behandelt.

6.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen einer Aufsichtsbehörde, soweit sie sich auf das Auftragsverhältnis beziehen.

§ 7 Rückgabe und Löschung

7.1 Nach Abschluss der Leistung gibt der Auftragnehmer alle personenbezogenen Daten aus dem Auftragsverhältnis nach Wahl des Auftraggebers zurück oder löscht sie. Der Auftraggeber teilt seine Wahl bei Vertragsende mit; ohne Mitteilung erfolgt die Löschung.

7.2 Gelöscht werden auch lokale Arbeitskopien, Testdatenbestände und Zugangsdaten.

7.3 Nachlauf der Sicherungen (Baustein 3). Der laufende Dienst und sein Datenbestand werden bei Vertragsende abgeschaltet und gelöscht. **Sicherungen** werden nicht einzeln bereinigt, sondern laufen nach **90 Tagen** ab; bis dahin bleiben sie verschlüsselt und zugriffsgeschützt und werden zu keinem anderen Zweck als der Wiederherstellung verwendet. Die vollständige Löschung ist damit 90 Tage nach Vertragsende abgeschlossen. Der Auftraggeber kann eine sofortige Löschung auch der Sicherungen verlangen; sie erfolgt dann unverzüglich.

7.4 Bestehen gesetzliche Aufbewahrungspflichten, bleiben die betreffenden Daten gespeichert; ihre Verarbeitung wird auf den Zweck der Aufbewahrung beschränkt.

7.5 Der Auftragnehmer bestätigt die Löschung auf Verlangen in Textform.

7.6 Übergang des Betriebs (Baustein 3). Endet der Vertrag, ohne dass der Betrieb eingestellt werden soll, stellt der Auftragnehmer dem Auftraggeber oder einem von diesem benannten Dritten die betriebsrelevanten Daten in einem gängigen, maschinenlesbaren Format bereit und unterstützt bei der Umstellung. Der Aufwand wird nach § 5.5 behandelt. Der Auftragnehmer schaltet den Dienst erst ab, wenn der Auftraggeber den Übergang bestätigt hat oder seit der Bereitstellung vier Wochen vergangen sind.

§ 8 Pflichten des Auftraggebers

8.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte betroffener Personen verantwortlich. Er stellt insbesondere sicher, dass für jede Verarbeitung eine Rechtsgrundlage nach Art. 6 DSGVO besteht.

8.2 Er teilt dem Auftragnehmer vor Beginn alle Umstände mit, die für die Verarbeitung erheblich sind, insbesondere einen der Fälle nach § 1.5.

8.3 Er stellt Berechtigungen nach § 3.3 bereit und entzieht sie unverzüglich, wenn sie nicht mehr erforderlich sind.

8.4 Für Test- und Entwicklungszwecke stellt er **keine echten personenbezogenen Daten** bereit. Ist das im Einzelfall unvermeidbar, vereinbaren die Parteien dies vorher in Textform und begrenzen den Umfang auf das

Notwendige.

8.5 Eigene Sicherung. Daten in seinen eigenen Systemen und Konten — auch in solchen, in denen der Auftragnehmer arbeitet, und in dem E-Mail-Postfach, in dem Nachrichten eines Kontaktformulars eingehen — sichert der Auftraggeber vor Beginn der Arbeiten und danach regelmäßig eigenverantwortlich. Bei Baustein 3 sichert der Auftragnehmer den Server nach § 3.10.

8.6 Inhalte und Formulare. Der Auftraggeber verantwortet, welche Angaben über Formulare und Eingabefelder seiner Websites und Anwendungen erhoben werden. Er verzichtet auf die Abfrage von Daten nach § 1.5 lit. a und b und weist Besucher darauf hin, solche Angaben nicht unaufgefordert zu übermitteln. Bei Baustein 4 gibt er in die KI-gestützten Funktionen keine Daten nach § 1.5 ein.

8.7 Datenschutzerklärung. Bei Baustein 3 stellt der Auftraggeber sicher, dass seine Datenschutzerklärung den Betrieb zutreffend beschreibt: den Auftragnehmer als Auftragsverarbeiter, die betreffenden Unterauftragsverarbeiter nach Anlage 3, den Serverstandort und die Speicherdauer der Protokolldateien. Der Auftragnehmer liefert ihm die dafür erforderlichen Angaben zu und teilt Änderungen unverzüglich mit.

§ 9 Haftung

9.1 Für die Haftung gilt Art. 82 DSGVO. Im Verhältnis der Parteien untereinander gelten ergänzend die Haftungsregelungen des Hauptvertrags.

9.2 Datenverlust. Für den Verlust von Daten aus einem nach Baustein 3 betriebenen Dienst ist die Haftung des Auftragnehmers auf den Aufwand beschränkt, der zur Wiederherstellung aus der letzten nach § 3.10 ordnungsgemäß erstellten Sicherung erforderlich ist, zuzüglich des Verlusts an Daten, die seit dieser Sicherung entstanden sind. Für Daten, die der Auftraggeber nach § 8.5 selbst sichert, ist die Haftung auf den Aufwand beschränkt, der bei ordnungsgemäßer und regelmäßiger eigener Sicherung zur Wiederherstellung erforderlich gewesen wäre. Beides gilt nicht bei Vorsatz und grober Fahrlässigkeit.

9.3 Klarstellung. Ansprüche betroffener Personen nach Art. 82 DSGVO gegen den Auftragnehmer werden durch Haftungsbegrenzungen des Hauptvertrags nicht berührt; solche Begrenzungen wirken ausschließlich im Verhältnis der Parteien zueinander.

§ 10 Laufzeit, Fassungen, Schlussbestimmungen

10.1 Der Vertrag läuft, solange der Hauptvertrag besteht. Eine gesonderte Kündigung ist ausgeschlossen; das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt für den Auftraggeber insbesondere vor, wenn der Auftragnehmer wesentliche Pflichten aus diesem Vertrag trotz Aufforderung nicht erfüllt.

10.2 Maßgebliche Fassung. Es gilt die Fassung dieses Vertrags, auf die das angenommene Angebot verweist. Spätere Angebote können auf eine neuere Fassung verweisen; mit deren Annahme gilt die neuere Fassung für das gesamte Auftragsverhältnis.

10.3 Veröffentlichung. Jede Fassung ist dauerhaft und unverändert unter `itservice-danieljacobs.de/rechtliches/avv/` mit ihrer Versionsnummer abrufbar (diese Fassung: `itservice-danieljacobs.de/rechtliches/avv/v4-1`). Die jeweils aktuelle Anlage 3 ist unter `itservice-danieljacobs.de/rechtliches/unterauftragsverarbeiter` abrufbar; frühere Stände bleiben dort einsehbar.

10.4 Sonstige Änderungen und Ergänzungen bedürfen der Textform. Das gilt auch für die Abbedingung dieses Formerfordernisses.

10.5 Ist eine Bestimmung unwirksam, bleibt die Wirksamkeit der übrigen unberührt.

10.6 Es gilt deutsches Recht. Gerichtsstand ist Nordhorn, soweit der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

§ 11 Abschluss

11.1 Dieser Vertrag kommt zustande, indem der Auftraggeber ein Angebot des Auftragnehmers annimmt, das auf diese Fassung verweist. Die Annahme in Textform, etwa per E-Mail, genügt (Art. 28 Abs. 9 DSGVO). Einer gesonderten Unterzeichnung bedarf es nicht.

11.2 Auf Wunsch einer Partei wird der Vertrag zusätzlich unterzeichnet. Für die Wirksamkeit ist dies nicht erforderlich.

11.3 Die Verarbeitung beginnt erst nach Abschluss dieses Vertrags.

Anlage 1 — Leistungsbausteine

Für einen Auftraggeber gelten nur die Bausteine, die in seinem Angebot genannt sind. Daten nach § 1.5 sind in keinem Baustein enthalten.

Baustein 1 — Arbeit an Systemen des Auftraggebers

Umfasst: Erstellung, Änderung, Wartung und Pflege von Websites und Software; Übernahme und Weiterentwicklung bestehender Software; Fehlersuche und Unterstützung; Bestandsaufnahme und Prüfung vorhandener Systeme; Installation und Pflege von Anwendungen auf Servern des Auftraggebers.

Wo: in den Systemen und Konten des Auftraggebers, Zugang nach Modell A oder B.

Betroffene Personen: Kunden, Interessenten, Lieferanten und deren Ansprechpartner, Besucher von Websites, Beschäftigte des Auftraggebers.

Datenarten: Stamm- und Kontaktdaten, Inhalte von Anfragen und Nachrichten, Vertrags- und Abrechnungsdaten, Nutzungs- und Protokolldaten, Zugangsdaten zu den Systemen des Auftraggebers — jeweils nur, soweit sie in den bearbeiteten Systemen vorhanden sind. Der Auftragnehmer greift auf diese Daten nur zu, soweit die Aufgabe es erfordert; er kopiert sie nicht in eigene Bestände, außer zur Fehlersuche im erforderlichen Umfang.

Baustein 2 — Schnittstellen und Datenmigration

Umfasst: Entwicklung und Betrieb von Schnittstellen zwischen Systemen des Auftraggebers; Übernahme von Daten aus einem Alt- in ein Neusystem; Datenbereinigung im Zuge der Übernahme.

Wo: in den Systemen des Auftraggebers; Zwischenstände der Migration lokal auf den Arbeitsgeräten des Auftragnehmers, verschlüsselt, und nur bis zum Abschluss der Migration.

Betroffene Personen und Datenarten: wie Baustein 1, zusätzlich Zahlungs- und Bankdaten, soweit sie Teil des übertragenen Bestands sind.

Besonderheit: Nach Abschluss der Migration löscht der Auftragnehmer alle Zwischenstände und bestätigt dies auf Verlangen in Textform.

Baustein 3 — Betrieb auf Infrastruktur des Auftragnehmers

Umfasst: Betrieb (Hosting) einer Website oder Anwendung des Auftraggebers auf einem Server des Auftragnehmers, einschließlich Bereitstellung, Aktualisierung, Absicherung, Überwachung und Datensicherung; Versand von Nachrichten aus Formularen an ein Postfach des Auftraggebers; Anmeldung der Nutzer des Auftraggebers an betriebenen Anwendungen.

Wo: auf dem Server und in den Sicherungen nach Anlage 3; Zugang nach Modell C.

Betroffene Personen: Besucher der Website, Kunden und Interessenten, die Formulare nutzen, Nutzer der betriebenen Anwendung (in der Regel Beschäftigte des Auftraggebers).

Datenarten: Nutzungs- und Protokolldaten (IP-Adresse, Zugriffszeitpunkt, abgerufene Ressource, Browser- und Systemangaben) — fallen beim Betrieb **immer** an; Inhalte von Formularen und Nachrichten; Termin- und Buchungsdaten, soweit die Website sie erhebt; Benutzerkonten der Nutzer (Name, dienstliche E-Mail-Adresse, Kennwort als Prüfwert, Anmeldezeitpunkte, Zweitfaktor).

Baustein 4 — KI-gestützte Funktionen in einer betriebenen Anwendung

Umfasst: Funktionen einer nach Baustein 3 betriebenen Anwendung, die Eingaben des Auftraggebers an einen KI-Anbieter nach Anlage 3 senden, etwa um Texte zu entwerfen, zu übersetzen oder zu überarbeiten. Nur zusammen mit Baustein 3.

Was übermittelt wird: die Inhalte, die der Nutzer der Funktion zur Bearbeitung übergibt (etwa Produktdaten, Stichpunkte, Bilder). Diese Funktionen sind **nicht** für personenbezogene Daten bestimmt. Personenbezug kann nur zufällig entstehen, etwa durch einen Namen in einem Freitext oder eine Person auf einem Foto.

Betroffene Personen: Nutzer der Anwendung; zufällig in Eingaben genannte oder abgebildete Personen.

Datenarten: Inhalte von Eingaben; keine Benutzerkonten, keine Protokolldaten.

Besonderheit: Der KI-Anbieter darf die Daten nach seinen Vertragsbedingungen nicht zum Training verwenden. Nutzt der Auftraggeber stattdessen einen **eigenen** Zugang bei einem KI-Anbieter, ist dieser Anbieter sein eigener Auftragsverarbeiter nach § 4.6, und dieser Baustein entfällt.

Baustein 5 — Unternehmensprofile bei Kartendiensten und Verzeichnissen

Umfasst: Einrichtung und Pflege des Unternehmensprofils des Auftraggebers bei Kartendiensten und Branchenverzeichnissen, einschließlich der Beantwortung von Bewertungen auf Weisung.

Wo: im Konto des Auftraggebers beim jeweiligen Anbieter, Zugang nach Modell A.

Betroffene Personen: Personen, die Bewertungen oder Fragen abgeben; Ansprechpartner des Auftraggebers.

Datenarten: öffentlich sichtbare Namen oder Kürzel der Bewertenden, Inhalte von Bewertungen und Fragen, geschäftliche Kontaktdaten.

Anlage 2 — Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO · Stand 09.10.2026

Das Gewerbe wird als Einzelunternehmen ohne Beschäftigte geführt. Der Auftragnehmer arbeitet in Systemen seiner Auftraggeber (Bausteine 1, 2 und 5) und **betreibt einen eigenen Server** in einem Rechenzentrum in

Deutschland (Bausteine 3 und 4). Die Maßnahmen beschreiben die Arbeitsgeräte und diesen Server.

1. Vertraulichkeit

Zutrittskontrolle. Die Arbeit erfolgt in abschließbaren Privaträumen ohne Publikumsverkehr. Der Server steht in einem Rechenzentrum des in Anlage 3 genannten Betreibers; für den physischen Zutritt gelten dessen Maßnahmen, die er durch Zertifikate nachweist. Der Auftragnehmer hat selbst keinen physischen Zugang.

Zugangskontrolle — Arbeitsgeräte. Alle Geräte sind passwortgeschützt und vollständig festplattenverschlüsselt. Automatische Bildschirmsperre nach kurzer Inaktivität. Betriebssystem und Anwendungen werden aktuell gehalten. Zwei-Faktor-Authentifizierung, wo angeboten. Persönliche Zugangsdaten liegen ausschließlich in einem verschlüsselten Passwortmanager. Dienstzugangsdaten, die der Betrieb dauerhaft braucht, liegen im Geheimnisspeicher des Bausystems und in einer Konfigurationsdatei auf dem Server außerhalb des ausgelieferten Verzeichnisses (§ 3.4 lit. a); sie stehen nicht in der Versionsverwaltung.

Zugangskontrolle — Server. Der Zugang erfolgt ausschließlich über SSH mit Schlüsselpaar; **die Anmeldung mit Passwort ist abgeschaltet, ebenso die Anmeldung als Administrator (root)**. Es besteht ein persönliches Konto mit Rechteerhöhung nach Bedarf. Eine Firewall lässt nur die betrieblich erforderlichen Anschlüsse zu. Dienste, die nicht aus dem Internet erreichbar sein müssen, lauschen ausschließlich auf der lokalen Netzwerkadresse.

Zugangskontrolle — betriebene Anwendungen. Anmeldung nur mit persönlichem Konto und Zweitfaktor. Kennwörter werden ausschließlich als Prüfwert nach aktuellem Stand der Technik gespeichert.

Getrennter Ausrollzugang. Für das Ausrollen neuer Stände besteht ein eigener, eingeschränkter Zugang, der ausschließlich ein festgelegtes Ausrollskript ausführen kann. Eine Befehlszeile steht über diesen Zugang nicht zur Verfügung.

Zugriffskontrolle. Zugriff besteht nur auf die Bestände, die für den Auftrag erforderlich sind. In Systemen des Auftraggebers arbeitet der Auftragnehmer, wo möglich, mit einem personengebundenen Konto mit den geringstmöglichen Rechten. Schnittstellenzugänge werden auf die benötigten Bereiche beschränkt.

Trennungskontrolle. Für jeden Auftraggeber wird ein eigenes Projektverzeichnis geführt. Auf dem Server läuft je Auftraggeber ein eigener, gekapselter Dienst (Container) mit eigenem Datenbestand, eigenen Zugangsdaten und eigener Konfiguration. Die Dienste können nicht auf die Datenbestände der jeweils anderen zugreifen.

Pseudonymisierung. Für Test- und Entwicklungszwecke werden anonymisierte oder pseudonymisierte Daten verwendet.

2. Integrität

Weitergabekontrolle. Übertragungen erfolgen ausschließlich verschlüsselt: HTTPS/TLS mit automatisch erneuerten Zertifikaten einer anerkannten Zertifizierungsstelle; SSH bei Serverzugriffen und beim Ausrollen; TLS beim E-Mail-Versand und bei der Übertragung an Unterauftragsverarbeiter. Ein Versand personenbezogener Daten per unverschlüsselter E-Mail findet nicht statt. Datenträger werden nicht versandt.

Eingabekontrolle. In Systemen des Auftraggebers wird über personengebundene Konten gearbeitet, sodass Änderungen zuordenbar bleiben. Änderungen am Quellcode sind über die Versionsverwaltung mit Zeitstempel und Urheber nachvollziehbar. Ausgerollt wird ausschließlich über den automatisierten Weg, sodass jeder Stand auf einen Stand der Versionsverwaltung zurückführbar ist. Eingriffe von Hand auf dem Server bleiben die Ausnahme und werden festgehalten.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle. Aktuelle Sicherheitsaktualisierungen, aktive Firewall, automatisierte Überwachung des Servers und der betriebenen Dienste. Die Überwachung meldet Zustandswechsel unverzüglich an den Auftragnehmer. Ergänzend prüft eine vom Server unabhängige Stelle regelmäßig von außen, ob die Dienste erreichbar sind.

Datensicherung. Mindestens tägliche, verschlüsselte Sicherung der betriebsrelevanten Daten an einen vom Server getrennten Ort bei einem anderen Anbieter als dem Rechenzentrumsbetreiber. Aufbewahrung **90 Tage**, danach automatische Löschung. Ein fehlgeschlagener Sicherungslauf wird als Fehler gemeldet und nicht stillschweigend übergangen. Arbeitsstände auf den Arbeitsgeräten werden regelmäßig verschlüsselt gesichert.

Wiederherstellbarkeit. Der Betriebsstand ist aus Versionsverwaltung und Sicherung wiederherstellbar. Ein früherer Stand eines Dienstes kann ohne Neubau zurückgeholt werden. Die Wiederherstellung aus einer Sicherung wird mindestens einmal jährlich erprobt und das Ergebnis festgehalten.

Protokolldateien. Zugriffsprotokolle des Webservers werden spätestens nach **acht Tagen** automatisch gelöscht. Sie dienen ausschließlich Sicherheit, Stabilität und Missbrauchserkennung, werden nicht mit anderen Quellen zusammengeführt und nicht zu Werbezwecken ausgewertet.

4. Verfahren zur Überprüfung und Bewertung

Auftragskontrolle. Verarbeitung nur auf Weisung. Die eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt; mit ihnen bestehen Verträge nach Art. 28 DSGVO.

Datenschutzmanagement. Ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO wird geführt und mindestens jährlich überprüft. Diese Maßnahmenbeschreibung wird im selben Turnus überprüft und bei Änderungen der Arbeitsweise angepasst.

Vorfallmanagement. Erkannte Verletzungen des Schutzes personenbezogener Daten werden dokumentiert und dem betroffenen Auftraggeber **innerhalb von 48 Stunden nach Kenntnis** gemeldet (§ 5.2).

Löschkonzept. Protokolldateien und Sicherungen laufen nach den oben genannten Fristen automatisch ab. Nach Auftragsende werden lokale Kopien, Testbestände, Zugangsdaten sowie Dienst und Datenbestand gelöscht, Sicherungen nach § 7.3. Datenträger werden vor der Entsorgung sicher gelöscht oder physisch zerstört.

Anlage 3 — Unterauftragsverarbeiter

Stand 09.10.2026 · aktuell abrufbar unter `itservice-danieljacobs.de/rechtliches/unterauftragsverarbeiter`

Ein Unterauftragsverarbeiter wird für einen Auftraggeber nur tätig, wenn dieser den genannten Baustein gebucht hat.

Nr.	Unterauftragsverarbeiter	Baustein	Zweck	Ort der Verarbeitung	Drittland / Grundlage
1	STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin	3	Serverbetrieb (Rechenzentrum)	Deutschland	kein Drittland

Nr.	Unterauftragsverarbeiter	Baustein	Zweck	Ort der Verarbeitung	Drittland / Grundlage
2	Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen (Dienst „Object Storage“)	3	Aufbewahrung der verschlüsselten Datensicherungen	Deutschland	kein Drittland
3	Mistral AI SAS, 15 rue des Halles, 75001 Paris, Frankreich	4	Entwerfen, Übersetzen und Überarbeiten von Texten aus Eingaben der Nutzer	EU	kein Drittland

Keine Unterauftragsverarbeiter — weil dort keine personenbezogenen Daten von Auftraggebern verarbeitet werden — sind:

- die Versionsverwaltung des Quellcodes (GitHub),
- der Dienst für Störungsmeldungen (ntfy.sh); die Meldungen enthalten Messwerte, keine Daten von Auftraggebern,
- KI-gestützte Arbeitswerkzeuge des Auftragnehmers für Entwicklung und Beratung (§ 4.7),
- Cloud-Ablagen für Angebote, Verträge und technische Unterlagen ohne Personenbezug.

Werden in diesen Diensten künftig personenbezogene Daten von Auftraggebern verarbeitet, wird der Dienst vorher nach § 4.2 in diese Liste aufgenommen.