

VEREINBARUNG ZUR

AUFTRAGSVERARBEITUNG

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Diese Vereinbarung wird abgeschlossen zwischen
dem Auftraggeber gemäß dem zugrunde liegenden Angebot bzw. Hauptvertrag
(Name bzw. Firma, Anschrift und Kontaktdaten ergeben sich aus dem Angebot bzw. Hauptvertrag)
– nachfolgend „Verantwortliche/r“ genannt –
und

Jonas Starck IT-Solutions

Einzelunternehmen, Inhaber: Jonas Starck
Mühlenweg 4, 4911 Tumeltsham, Österreich
E-Mail: starck.it.solutions@gmail.com
Tel: +43 681 10898118

Web: <https://www.starckitsolutions.at>

– nachfolgend „Auftragsverarbeiter“ genannt –
– gemeinsam die „Parteien“ –

§ 1 Gegenstand und Grundlage

(1) Der Auftragsverarbeiter erbringt für den/die Verantwortliche/n Leistungen in den Bereichen Webentwicklung, Entwicklung mobiler Applikationen (iOS/Android), Backend- und Schnittstellen-Entwicklung (APIs), technische Betreuung, Wartung und Hosting von Websites und Web-Anwendungen – jeweils in dem Umfang, in dem diese Leistungen im Einzelfall gemäß Hauptvertrag bzw. Beauftragung vereinbart sind. Im Rahmen dieser Tätigkeit erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten, die der/die Verantwortliche als datenschutzrechtlich Verantwortliche/r im Sinne des Art. 4 Nr. 7 DSGVO verarbeitet.

(2) Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des/der Verantwortlichen und gilt für alle Tätigkeiten, bei denen Beschäftigte des Auftragsverarbeiters oder von ihm beauftragte Dritte personenbezogene Daten des/der Verantwortlichen verarbeiten.

(3) Die Regelungen dieser Vereinbarung gehen den Bestimmungen des zugrunde liegenden Hauptvertrags (Dienstleistungs-/Werkvertrag) im Hinblick auf den Datenschutz vor.

(4) Diese Vereinbarung wird durch Einbeziehung in das Angebot bzw. den Hauptvertrag des Auftragsverarbeiters mit dessen Annahme durch den/die Verantwortliche/n in Textform wirksam. Einer gesonderten Unterzeichnung dieser Vereinbarung bedarf es nicht (Art. 28 Abs. 9 DSGVO). Maßgeblich ist die im Angebot bzw. Hauptvertrag bezeichnete Fassung (Stand siehe Ende dieses Dokuments).

§ 2 Gegenstand, Art und Zweck der Verarbeitung, Dauer

(1) Art und Zweck der Verarbeitung: Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zum Zweck der Erbringung folgender Leistungen für den/die Verantwortliche/n – jeweils soweit im Einzelfall gemäß Hauptvertrag beauftragt:

- Erstellung, Einrichtung und Weiterentwicklung von Websites und Web-Anwendungen (Webentwicklung);
- Entwicklung und Pflege mobiler Applikationen (iOS/Android) sowie Backend- und Schnittstellen-Entwicklung (APIs);
- technische Wartung, Pflege, Updates und Fehlerbehebung;
- Bereitstellung bzw. Verwaltung des Hostings (über den Auftragsverarbeiter, siehe § 7);
- unterstützende Tätigkeiten bei der Verwaltung von Inhalten, soweit die/der Verantwortliche dies im Einzelfall anfordert.

(2) E-Commerce- bzw. Online-Shop-Leistungen sowie die Verarbeitung von Zahlungs- und Bestelldaten sind nicht Gegenstand dieser Vereinbarung und werden vom Auftragsverarbeiter nicht erbracht.

(3) Dauer: Diese Vereinbarung wird auf unbestimmte Zeit geschlossen und läuft, solange der Auftragsverarbeiter Leistungen gemäß dem Hauptvertrag erbringt. Sie endet automatisch mit Beendigung des Hauptvertrags, unbeschadet fortbestehender Löschungs- und Rückgabepflichten gemäß § 8.

§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Art der verarbeiteten personenbezogenen Daten (je nach beauftragtem Leistungsumfang):

- Stammdaten (Vor- und Nachname, ggf. Firmenname, ggf. UID-Nummer);
- Kontaktdaten (Anschrift, E-Mail-Adresse, Telefonnummer);
- Vertrags- und Kommunikationsdaten (Inhalt von Anfragen, Korrespondenz, Support-Tickets);
- Konto- und Zugangsdaten (bei Benutzerkonten, z. B. Benutzername, verschlüsseltes Passwort);
- Inhaltsdaten, die der/die Verantwortliche zur Veröffentlichung oder Verarbeitung bereitstellt (z. B. Texte, Bilder, Dokumente);
- Nutzungs- und Server-Logdaten (z. B. IP-Adresse, Zugriffszeitpunkt) im Rahmen des Hostings.

(2) Kategorien betroffener Personen:

- Kundinnen und Kunden sowie Interessentinnen und Interessenten des/der Verantwortlichen;
- Nutzerinnen und Nutzer der Website bzw. Web-Anwendung;
- Kontaktpersonen (z. B. über das Kontaktformular).

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des/der Verantwortlichen, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet. In einem solchen Fall teilt er dem/der Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragsverarbeiter informiert den/die Verantwortliche/n unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen sonstige Datenschutzbestimmungen verstößt.

(3) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(4) Der Auftragsverarbeiter ergreift alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (siehe § 6 und Anlage 1).

(5) Der Auftragsverarbeiter unterstützt den/die Verantwortliche/n nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte (Art. 12–23 DSGVO) sowie bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO.

(6) Der Auftragsverarbeiter meldet dem/der Verantwortlichen jede Verletzung des Schutzes personenbezogener

Daten unverzüglich nach Bekanntwerden, damit diese/r ihren/seinen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO nachkommen kann.

(7) Der Auftragsverarbeiter stellt dem/der Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen (siehe § 9).

§ 5 Rechte und Pflichten des/der Verantwortlichen

(1) Der/die Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich (Art. 4 Nr. 7, Art. 24 DSGVO).

(2) Der/die Verantwortliche erteilt Weisungen grundsätzlich in Textform (z. B. per E-Mail). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der/die Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er/sie Fehler oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten feststellt.

§ 6 Technische und organisatorische Maßnahmen (TOM)

(1) Der Auftragsverarbeiter trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen nach dem Stand der Technik, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO).

(2) Die Maßnahmen können im Laufe des Vertragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, solange das vereinbarte Schutzniveau nicht unterschritten wird.

§ 7 Sub-Auftragsverarbeiter

(1) Der/die Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Einschaltung von Sub-Auftragsverarbeitern. Die zum Zeitpunkt des Vertragsschlusses eingesetzten bzw. je nach beauftragtem Leistungsumfang einsetzbaren Sub-Auftragsverarbeiter sind in Anlage 2 aufgeführt; die Liste wird bei Änderungen gemäß Abs. 2 aktualisiert und bedarf keiner erneuten Unterzeichnung dieser Vereinbarung.

(2) Der Auftragsverarbeiter darf weitere Sub-Auftragsverarbeiter hinzuziehen oder bestehende ersetzen, sofern er den/die Verantwortliche/n vorab in Textform informiert und ihm/ihr ein Widerspruchsrecht innerhalb einer angemessenen Frist einräumt. Erfolgt innerhalb dieser Frist kein Widerspruch aus wichtigem, datenschutzrechtlich begründetem Anlass, gilt die Zustimmung als erteilt.

(3) Der Auftragsverarbeiter verpflichtet jeden Sub-Auftragsverarbeiter durch Vertrag auf dieselben Datenschutzpflichten, die in dieser Vereinbarung festgelegt sind, insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO).

(4) Hinweis zum Hosting: Soweit Hosting beauftragt ist, erfolgt dieses über einen Vertrag des Auftragsverarbeiters mit einem Hosting-Anbieter (siehe Anlage 2). Der jeweilige Hosting-Anbieter ist damit Sub-Auftragsverarbeiter des Auftragsverarbeiters. Der Auftragsverarbeiter hat mit dem jeweiligen Hosting-Anbieter einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO abgeschlossen.

(5) Übermittlung in Drittländer: Eine Verarbeitung personenbezogener Daten in einem Drittland außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Dies ist insbesondere der Fall, wenn für das betreffende Drittland ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt (z. B. eine Zertifizierung des Empfängers nach dem EU-U.S. Data Privacy Framework) oder geeignete Garantien gemäß Art. 46 DSGVO vereinbart wurden, insbesondere Standardvertragsklauseln der Europäischen Kommission, erforderlichenfalls ergänzt um zusätzliche Schutzmaßnahmen. Dies gilt auch für den Einsatz von Sub-Auftragsverarbeitern mit Sitz oder Verarbeitungsstandorten in Drittländern sowie für Fälle, in denen Sub-Auftragsverarbeiter mit Sitz in der EU/im

EWR ihrerseits Unterauftragsverarbeiter in Drittländern einsetzen.

§ 8 Löschung und Rückgabe von Daten

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des/der Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück, sofern nicht nach Unionsrecht oder dem Recht eines Mitgliedstaats eine Verpflichtung zur Speicherung besteht.

(2) Bestehende gesetzliche Aufbewahrungspflichten des/der Verantwortlichen (insbesondere steuer- und handelsrechtliche Fristen, in Österreich i. d. R. sieben Jahre gemäß § 132 BAO) bleiben unberührt.

(3) Die Löschung ist dem/der Verantwortlichen auf Anforderung in geeigneter Form zu bestätigen.

§ 9 Nachweis- und Kontrollrechte

(1) Der Auftragsverarbeiter weist die Einhaltung der in dieser Vereinbarung festgelegten Pflichten auf Anforderung in geeigneter Weise nach.

(2) Der/die Verantwortliche ist berechtigt, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Kontrollen sind rechtzeitig anzukündigen, auf das erforderliche Maß zu beschränken und so durchzuführen, dass der Geschäftsbetrieb des Auftragsverarbeiters möglichst wenig beeinträchtigt wird.

§ 10 Haftung

(1) Für die Haftung gilt Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei für Schäden, die durch eine von ihr zu vertretende Verletzung dieser Vereinbarung oder der datenschutzrechtlichen Bestimmungen verursacht werden.

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für die Änderung dieser Klausel.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien verpflichten sich, eine unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen und datenschutzrechtlichen Zweck am nächsten kommt.

(3) Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen des internationalen Privatrechts und des UN-Kaufrechts.

(4) Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen im Hinblick auf den Datenschutz die Regelungen dieser Vereinbarung vor.

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die nachfolgend beschriebenen Maßnahmen geben den Stand zum Zeitpunkt des Vertragsschlusses wieder. Der Auftragsverarbeiter ist berechtigt und verpflichtet, die Maßnahmen entsprechend der technischen Weiterentwicklung und der Risikolage fortlaufend anzupassen und zu verbessern (§ 6 Abs. 2 dieser Vereinbarung). Einzelne Maßnahmen dürfen dabei durch gleichwertige oder wirksamere ersetzt werden, solange das vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Eine Aktualisierung dieser Anlage bedarf keiner erneuten Unterzeichnung dieser Vereinbarung; die jeweils aktuelle Fassung wird dem/der Verantwortlichen auf Anforderung zur Verfügung gestellt.

Zutrittskontrolle

- Verarbeitung überwiegend remote; Arbeitsgeräte in gesicherten Räumlichkeiten

- Server-Infrastruktur in zertifizierten Rechenzentren des Hosting-Anbieters (EU)

Zugangskontrolle

- Individuelle Benutzerkonten mit starken Passwörtern
- Einsatz eines verschlüsselten Passwort-Managers (Zero-Knowledge-Verschlüsselung, EU-Server) zur sicheren Generierung, Verwaltung und Speicherung komplexer Passwörter
- Sperrung von Zugängen bei Inaktivität / Ausscheiden

Zugriffskontrolle

- Rollen- und Berechtigungskonzept (need-to-know-Prinzip)
- Beschränkung administrativer Zugriffe auf das erforderliche Maß

Weitergabekontrolle

- Verschlüsselte Datenübertragung (TLS/HTTPS)
- Keine Übertragung personenbezogener Daten über unverschlüsselte Kanäle

Eingabekontrolle

- Getrennte Benutzerkonten je bearbeitender Person
- Nachvollziehbarkeit von Änderungen über Versionsverwaltung, soweit technisch möglich

Verfügbarkeitskontrolle

- Schutz vor Schadsoftware (Firewall, Security-Plugins)
- Regelmäßige Updates von System- und Anwendungssoftware
- Regelmäßige Backups im Rahmen des beauftragten Hostings

Trennungskontrolle

- Logische Mandantentrennung je Kundenprojekt

Belastbarkeit & Wiederherstellung

- Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der eingesetzten Sicherheitsmaßnahmen

Anlage 2 – Genehmigte Sub-Auftragsverarbeiter

Die nachfolgende Liste gibt die vom Auftragsverarbeiter eingesetzten Sub-Auftragsverarbeiter zum Zeitpunkt des Vertragsschlusses wieder (Stand: siehe unten). Sie erhebt keinen Anspruch auf dauerhafte Vollständigkeit: Der Auftragsverarbeiter ist gemäß § 7 dieser Vereinbarung berechtigt, Sub-Auftragsverarbeiter hinzuzuziehen, zu ersetzen oder deren Einsatz zu beenden. Über beabsichtigte Änderungen wird der/die Verantwortliche vorab in Textform informiert und kann ihnen innerhalb von 14 Tagen aus wichtigem, datenschutzrechtlich begründetem Anlass widersprechen. Eine Aktualisierung dieser Anlage bedarf keiner erneuten Unterzeichnung dieser Vereinbarung. Die Liste umfasst sämtliche Sub-Auftragsverarbeiter, die je nach beauftragtem Leistungsumfang zum Einsatz kommen können; ob und welche im Einzelfall tatsächlich eingesetzt werden, richtet sich nach den gemäß Hauptvertrag beauftragten Leistungen.

Hetzner Online GmbH

Anschrift: Industriestraße 25, 91710 Gunzenhausen, Deutschland (Verarbeitung in deutschen Rechenzentren)
Zweck: Hosting, Server- und Infrastrukturdienstleistungen – Einsatz nur bei Hosting über den Auftragsverarbeiter.

Dynadot LLC

Anschrift: 210 S Ellsworth Ave #345, San Mateo, CA 94401, USA
Zweck: Domain-Registrierung und DNS-Verwaltung – Einsatz nur bei Domainverwaltung über den Auftragsverarbeiter. Datenübermittlung in die USA auf Grundlage geeigneter Garantien gemäß Art. 44 ff. DSGVO.

Google Ireland Ltd.

Anschrift: Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland

Zweck: E-Mail- und Kommunikationsdienst (Gmail / Google Workspace) zur Abwicklung der Kundenkommunikation

– Einsatz in allen Leistungsbereichen.

Anlage 3 – Genehmigte Systemzugriffe

Der Auftragsverarbeiter erhält zur Leistungserbringung Zugriff auf Systeme und Konten des/der Verantwortlichen, insbesondere auf die nachfolgend beispielhaft aufgeführten. Die Aufzählung ist nicht abschließend; Zugriff auf weitere Systeme kann im Rahmen der Leistungserbringung nach Abstimmung in Textform erfolgen. Sämtliche Zugriffe erfolgen ausschließlich auf Weisung und im Interesse des/der Verantwortlichen. Die aufgeführten Systeme kommen je nach beauftragtem Leistungsumfang in Betracht; ein Zugriff erfolgt nur, soweit er für die jeweils beauftragten Leistungen erforderlich ist.

Content-Management-System / Website- bzw. Anwendungs-Backend

Beispiele: z. B. WordPress-Administration, Headless-CMS, Angular- bzw. .NET-Adminbereiche

Zweck und Umfang: Erstellung, Wartung, Pflege, Updates und Fehlerbehebung der Website bzw. Web-Anwendung; unterstützende Verwaltung von Inhalten auf Anforderung.

Hosting-Umgebung / Server / Domainverwaltung des Kunden

Beispiele: z. B. kundeneigene Hosting-, Server- oder Domain-Zugänge, Cloud-Konsolen (z. B. Oracle Cloud)

Zweck und Umfang: Einrichtung und Verwaltung des Hostings, Server-Konfiguration, Backups, SSL-Zertifikate, Domain- und E-Mail-Einstellungen.

Repository- und Deployment-Systeme

Beispiele: z. B. Git-Repositories, CI/CD-Pipelines, App-Build-Systeme

Zweck und Umfang: Entwicklung, Versionsverwaltung und Auslieferung von Websites und Anwendungen.

App-Store- und Entwickler-Konten des Kunden

Beispiele: z. B. Apple App Store Connect, Google Play Console

Zweck und Umfang: Veröffentlichung und Pflege mobiler Applikationen im Auftrag des Kunden, soweit beauftragt.

Marketing-, Funnel- und Analyse-Tools des Kunden

Beispiele: z. B. Newsletter-Systeme, Statistik- und Analyse-Tools

Zweck und Umfang: Einrichtung, Konfiguration und Auswertung, soweit im Einzelfall beauftragt.

Stand dieser Vereinbarung: September 2026