Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO · haushalt.cloud · Stand 27.10.2026

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO für die Nutzung von Haushalt Planspiel unter haushalt.cloud – mit technischen und organisatorischen Maßnahmen und der Liste der Unterauftragsverarbeiter.

Vertragsparteien

Verantwortlicher: die im Bestellformular genannte Kommune bzw. Einrichtung (im Folgenden „Verantwortlicher“).

Auftragsverarbeiter: Haushalt.cloud UG (haftungsbeschränkt) i. G., vertreten durch den Geschäftsführer Frank Lewandowski, Weinheimer Weg 42, 68623 Lampertheim · vertrieb@haushalt.cloud · +49 6206 3056519 (im Folgenden „Auftragsverarbeiter“).

§ 1 Gegenstand und Dauer

1. Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen bei der Bereitstellung von Haushalt Planspiel als Software as a Service (Hauptvertrag: Bestellung nach den AGB des Auftragsverarbeiters oder Vertrag nach EVB-IT Cloud).
2. Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Pflichten zur Löschung und Rückgabe nach § 9 gelten über das Vertragsende hinaus.

§ 2 Art, Zweck und Umfang der Verarbeitung

1. Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.
2. Die Verarbeitung findet grundsätzlich in Deutschland statt. Eine Übermittlung in ein Drittland erfolgt nur im Rahmen der in Anlage 3 genannten Unterauftragsverarbeiter und nur unter den Voraussetzungen der Art. 44 ff. DSGVO (§ 6).
3. Die vom Verantwortlichen übermittelten Haushaltsdaten sind zusammengefasste Finanzkennzahlen ohne Personenbezug. Der Stellenplan enthält ausschließlich Stellenzahlen. Diese Daten fallen nicht unter diesen Vertrag, solange sie keinen Personenbezug aufweisen.

§ 3 Weisungsbefugnis

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder deutschem Recht zur Verarbeitung verpflichtet. In diesem Fall teilt er dem Verantwortlichen diese Anforderung vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.
2. Weisungen erteilt der Verantwortliche in Textform, vorzugsweise über ein Ticket im Kundenbereich oder per E-Mail an support@haushalt.cloud. Mündliche Weisungen bestätigt der Verantwortliche unverzüglich in Textform.
3. Weisungsberechtigt sind die im Kundenbereich hinterlegten Ansprechpersonen des Verantwortlichen. Weisungsempfänger beim Auftragsverarbeiter ist Frank Lewandowski, Geschäftsführer.
4. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, weist er den Verantwortlichen unverzüglich darauf hin. Er darf die Ausführung bis zur Bestätigung oder Änderung der Weisung aussetzen.

§ 4 Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verpflichtet alle Personen, die Zugang zu personenbezogenen Daten haben, zur Vertraulichkeit, soweit sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen.

2. Er trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Anlage 2. Er darf die Maßnahmen weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er.
3. Er unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Beantwortung von Anträgen betroffener Personen nach Art. 12 bis 23 DSGVO. Wendet sich eine betroffene Person direkt an ihn, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter.
4. Er unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei Datenschutz-Folgenabschätzungen und Meldungen an die Aufsichtsbehörde.
5. Verletzungen des Schutzes personenbezogener Daten meldet er dem Verantwortlichen unverzüglich, innerhalb von 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt.
6. Ansprechpartner für den Datenschutz beim Auftragsverarbeiter: Frank Lewandowski, vertrieb@haushalt.cloud, +49 6206 3056519.

---

§ 5 Unterauftragsverarbeiter

1. Der Verantwortliche erteilt die allgemeine Genehmigung zur Beauftragung von Unterauftragsverarbeitern. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 3 genannt und gelten als genehmigt.
2. Der Auftragsverarbeiter informiert den Verantwortlichen mindestens vier Wochen vor der Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist widersprechen. Kommt keine Einigung zustande, können beide Parteien den Hauptvertrag zum Zeitpunkt der Änderung kündigen.
3. Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein Datenschutzniveau, das diesem Vertrag entspricht.
4. Keine Unterauftragsverarbeitung sind Nebenleistungen wie Telekommunikation, Post- und Transportdienste oder die Wartung von Hardware, soweit dabei kein Zugriff auf personenbezogene Daten des Verantwortlichen erfolgt.

---

§ 6 Drittlandübermittlung

1. Eine Übermittlung personenbezogener Daten in ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, etwa durch einen Angemessenheitsbeschluss oder Standardvertragsklauseln.
2. Die jeweilige Grundlage ist in Anlage 3 beim betreffenden Unterauftragsverarbeiter angegeben.

---

§ 7 Kontrollrechte

1. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind.
2. Der Verantwortliche oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer kann die Einhaltung nach Ankündigung mit einer Frist von zwei Wochen während der üblichen Geschäftszeiten überprüfen, ohne den Betriebsablauf unverhältnismäßig zu stören.
3. Der Nachweis kann auch durch aktuelle Testate, Zertifikate oder Prüfberichte unabhängiger Stellen, etwa des Hosting-Anbieters, erbracht werden.

---

§ 8 Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Rechte betroffener Personen verantwortlich.
2. Er informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.
3. Er übermittelt keine personenbezogenen Daten, die für die Leistung nicht erforderlich sind, insbesondere keine Namen von Beschäftigten in Haushalts- oder Stellenplandaten.

§ 9 Löschung und Rückgabe

1. Nach Ende des Hauptvertrags gibt der Auftragsverarbeiter auf Wunsch des Verantwortlichen die von diesem übermittelten Daten in einem gängigen Dateiformat heraus.
2. Anschließend, spätestens einen Tag nach Vertragsende, löscht er alle personenbezogenen Daten des Verantwortlichen, insbesondere die Daten des Kundenbereichs (sofern genutzt) und die Dateien der Planspiel-Instanz, sofern keine gesetzliche Pflicht zur Speicherung besteht, und bestätigt die Löschung auf Anfrage in Textform.
3. Daten in Datensicherungen werden im Rahmen der regulären Rotation spätestens nach 7 Tagen gelöscht.

§ 10 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis gelten die Haftungsregeln des Hauptvertrags, soweit Art. 82 DSGVO nichts anderes bestimmt.

§ 11 Schlussbestimmungen

1. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag geht dieser Vertrag in Fragen des Datenschutzes vor.
2. Änderungen und Ergänzungen bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
3. Es gilt das Recht der Bundesrepublik Deutschland.
4. Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlage 1 - Gegenstand der Verarbeitung

Die Verarbeitung dient der Bereitstellung, dem sicheren Betrieb und dem Support der Planspiel-Instanz des Verantwortlichen.

Bereich	Betroffene Personen	Datenarten	Zweck
Planspiel-Instanz	Teilnehmende	IP-Adresse und Verbindungsdaten (Server-Logfiles und Web Application Firewall, Löschung nach 7 Tagen), eingegebener Sessioncode. Spielentscheidungen und Spielstand werden ausschließlich lokal im Browser verarbeitet und nicht auf dem Server gespeichert	Bereitstellung des Planspiels, Zugangsprüfung, Abwehr von Angriffen
Kundenbereich login.haushalt.cloud	Ansprechpersonen und Nutzende des Verantwortlichen	Name, Funktion, E-Mail, Telefon; öffentlicher Schlüssel und Gerätebezeichnung des Passkeys; E-Mail für Login-Links; Anmeldeprotokolle mit Zeitpunkt und IP-Adresse; freigegebene IP-Adressen bzw. Tailscale-Gerätekennungen	Anmeldung, Zugriffsbeschränkung, Verwaltung der Instanz, Missbrauchserkennung
Support	Ansprechpersonen des Verantwortlichen	Name, E-Mail, Telefonnummer, Inhalte von Tickets, E-Mails und Telefonaten	Bearbeitung von Anfragen und Weisungen

Bereich	Betroffene Personen	Datenarten	Zweck
Inhalte des Verantwortlichen	ggf. in Logos oder Texten genannte Personen	Logo, Wappen, Farben, Texte	Darstellung der Instanz im Erscheinungsbild des Verantwortlichen

Verarbeitungsarten: Erheben, Speichern, Anzeigen, Abgleichen, Übermitteln an Unterauftragsverarbeiter, Löschen.

Anlage 2 - Technische und organisatorische Maßnahmen

Vertraulichkeit

- Zutritt: Betrieb ausschließlich in Rechenzentren des Hosting-Anbieters in Deutschland; physische Sicherung durch die STRATO GmbH; Nachweise des Hosting-Anbieters auf Anfrage.
- Zugang: Kundenbereich mit Passkey oder einmaligem Login-Token, keine Passwörter; erreichbar nur über freigegebene IP-Adressen oder Tailscale; administrative Zugänge ausschließlich per Passkey (Hardware-Sicherheitsschlüssel YubiKey oder Smartphone).
- Zugriff: durchgängiges Berechtigungskonzept; Zugriff auf Kundendaten nur für Personen, die ihn für Betrieb und Support benötigen.
- Trennung: eigene Instanz je Kunde in einem eigenen Container unter eigener Subdomain.
- Datensparsamkeit: Teilnehmende spielen ohne Registrierung und ohne Namen; ein Sessioncode je Instanz statt persönlicher Konten; Spielstände nur lokal im Browser, keine Speicherung auf dem Server.

Integrität

- Verschlüsselte Übertragung aller Verbindungen per TLS.
- Protokollierung von Anmeldungen im Kundenbereich mit Zeitpunkt und IP-Adresse.
- Änderungen an Haushaltsdaten erst nach Prüfung durch das Team des Auftragsverarbeiters.

Verfügbarkeit und Belastbarkeit

- Web Application Firewall vor allen öffentlichen Diensten; IP-Adressen, von denen aktive Angriffe ausgehen, werden für 72 Stunden gesperrt.
- Laufende Überwachung von Erreichbarkeit, Diensten und Zertifikaten.
- Tägliche Datensicherung der Container und der Datenbank mit Speicherort in Deutschland; Aufbewahrung der Sicherungen 7 Tage; wöchentliche Wiederherstellungstests im Rahmen des Disaster-Recovery-Plans.

Verfahren zur regelmäßigen Überprüfung

- Zentrale Updates und Sicherheitsaktualisierungen ohne Aufwand für den Verantwortlichen.
- Monatliches Audit der Maßnahmen sowie anlassbezogene Überprüfung nach Sicherheitsvorfällen.
- Verfahren für Datenschutzvorfälle mit Meldung an den Verantwortlichen nach § 4 Abs. 5.

Anlage 3 - Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Grundlage bei Drittland
STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin	Hosting, Rechenzentrum, Datensicherung	Deutschland	entfällt

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Grundlage bei Drittland
STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin	Versand von Login-Links und Benachrichtigungen	Deutschland	entfällt
Tailscale Inc.	Gesicherter Zugang zum Kundenbereich, nur bei Nutzung von Tailscale	Europa	EU-Standardvertragsklauseln, soweit Daten außerhalb der EU/des EWR verarbeitet werden

Haushalt.cloud UG (haftungsbeschränkt) i. G. · Weinheimer Weg 42 · 68623 Lampertheim

vertrieb@haushalt.cloud · +49 6206 3056519 · haushalt.cloud

Sitz: Lampertheim · Handelsregister: Eintragung beim Amtsgericht Darmstadt ausstehend · Geschäftsführer: Frank Lewandowski · USt-IdNr. angefordert