Vertrag über die Auftragsverarbeitung

nach Art. 28 DSGVO · Fassung 1.0 vom 18. September 2026

Vertragsparteien

Dieser Vertrag wird geschlossen zwischen dem Kunden als Verantwortlichem (im Folgenden „Auftraggeber“) und

datheon IT-Systemhaus UG (haftungsbeschränkt), Gifhorner Straße 152, 38112 Braunschweig, vertreten durch Tim Jahn, als Auftragsverarbeiter (im Folgenden „Auftragnehmer“).

Er ergänzt den Nutzungsvertrag über die Plattform Branchway (Allgemeine Geschäftsbedingungen, im Folgenden „Hauptvertrag“) und gilt, solange der Auftragnehmer im Rahmen des Hauptvertrags personenbezogene Daten im Auftrag verarbeitet.

§ 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber eine Plattform zum Betrieb von Webanwendungen bereit: Ausführung von Anwendungen (Apps und Funktionen), verwaltete Datenbanken, Dateispeicher, Protokolle und Sicherungen. Dabei verarbeitet er personenbezogene Daten, die der Auftraggeber oder die Nutzer seiner Anwendungen dort ablegen.

Die Verarbeitung besteht im Speichern, Aufbewahren, Sichern, Übermitteln innerhalb der Plattform, Ausführen des Codes des Auftraggebers auf diesen Daten und Löschen. Eine inhaltliche Auswertung der Daten durch den Auftragnehmer findet nicht statt.

Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags.

§ 2 Art der Daten und Kreis der Betroffenen

Welche Daten verarbeitet werden, bestimmt allein der Auftraggeber durch den Inhalt seiner Anwendungen, Datenbanken und Dateien. Typischerweise sind das:

- Bestands- und Kontaktdaten (etwa Name, Anschrift, E-Mail-Adresse, Telefonnummer)
- Vertrags-, Bestell- und Zahlungsdaten der Kunden des Auftraggebers
- Nutzungs- und Verbindungsdaten (etwa IP-Adressen, Zeitpunkte, Protokolleinträge der Anwendungen)
- Inhalte, die Nutzer hochladen oder eingeben (Texte, Bilder, Dokumente)
- Betroffen sind Kunden, Interessenten, Nutzer, Beschäftigte und Kontaktpersonen des Auftraggebers.
- Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) verarbeitet der Auftraggeber nur, wenn er selbst die dafür nötigen zusätzlichen Schutzmaßnahmen prüft und verantwortet.

§ 3 Weisungen des Auftraggebers

Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Weisungen sind der Hauptvertrag, dieser Vertrag und die Einstellungen, die der Auftraggeber in der Console oder über die Programmierschnittstelle vornimmt (etwa Anlegen, Ändern und Löschen von Apps, Datenbanken, Dateien und Sicherungen).

Ist der Auftragnehmer gesetzlich zu einer anderen Verarbeitung verpflichtet, teilt er dem Auftraggeber das vorher mit, sofern das Gesetz eine solche Mitteilung nicht verbietet.

Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber unverzüglich darauf hin und darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

§ 4 Vertraulichkeit

Der Auftragnehmer setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Zugriff auf Daten des Auftraggebers erhalten sie nur, soweit das für den Betrieb, die Fehlerbehebung oder auf Anfrage des Auftraggebers nötig ist.

§ 5 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in Anlage 1 beschriebenen Maßnahmen nach Art. 32 DSGVO. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt; wesentliche Änderungen dokumentiert er in einer neuen Fassung dieses Vertrags.

Für die Sicherheit des eigenen Codes, der eigenen Zugangsdaten und der Rechtevergabe innerhalb seines Teams ist der Auftraggeber selbst verantwortlich.

§ 6 Unterauftragsverarbeiter

Der Auftraggeber genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter. Der Auftragnehmer verpflichtet sie vertraglich auf ein Schutzniveau, das diesem Vertrag entspricht.

Über die Hinzunahme oder den Austausch eines Unterauftragsverarbeiters informiert der Auftragnehmer mindestens 30 Tage vorher per E-Mail an die Inhaber des Teams. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen; kommt keine Einigung zustande, darf er den Hauptvertrag zum Zeitpunkt der Änderung kündigen.

Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet nicht statt.

§ 7 Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Beantwortung von Anfragen betroffener Personen (Art. 12 bis 23 DSGVO), bei der Sicherheit der Verarbeitung, bei Meldungen von Datenschutzverletzungen und bei Datenschutz-Folgenabschätzungen (Art. 32 bis 36 DSGVO).

Da der Auftraggeber seine Daten selbst über die Console und die Schnittstellen einsehen, ändern, exportieren und löschen kann, erfüllt er Auskunfts-, Berichtigungs- und Löschanfragen in der Regel selbst. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser die Anfrage unverzüglich weiter.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, über eine Verletzung des Schutzes personenbezogener Daten, die Daten des Auftraggebers betrifft. Die Meldung enthält, soweit bekannt, Art und Umfang der Verletzung, die betroffenen Datenkategorien, die wahrscheinlichen Folgen und die ergriffenen Gegenmaßnahmen.

§ 9 Löschung und Rückgabe nach Vertragsende

Der Auftraggeber kann seine Daten während der Vertragslaufzeit jederzeit selbst exportieren. Nach Ende des Hauptvertrags löscht der Auftragnehmer die Daten des Auftraggebers einschließlich der Sicherungen spätestens nach 30 Tagen, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Rechnungs- und Abrechnungsdaten des Auftraggebers selbst sind davon ausgenommen; sie unterliegen den handels- und steuerrechtlichen Aufbewahrungsfristen.

§ 10 Nachweise und Kontrollen

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags nötig sind. Kontrollen vor Ort sind nach rechtzeitiger Anmeldung, in der Regel mit einer Frist von vier Wochen, während der Geschäftszeiten möglich, soweit sie den Betrieb und die Vertraulichkeit anderer Kunden nicht gefährden. Nachweise der Rechenzentrumsbetreiber (etwa Zertifizierungen) gelten als Nachweis für deren Bereich.

§ 11 Schlussbestimmungen

Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag geht dieser Vertrag in Fragen des Datenschutzes vor. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam. Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, der Sitz des Auftragnehmers.

Dieser Vertrag wird elektronisch geschlossen. Abschluss, Version und Zeitpunkt werden beim Auftragnehmer

gespeichert und sind für den Auftraggeber in der Console einsehbar.

Anlage 1: Technische und organisatorische Maßnahmen

Stand der Maßnahmen: Fassung 1.0 vom 18. September 2026.

- Standort: Alle Server und Sicherungen befinden sich in Rechenzentren in Deutschland.
- Zutrittskontrolle: Der physische Zutritt zu den Servern wird durch den Rechenzentrumsbetreiber (Anlage 2) nach dessen Sicherheitskonzept und Zertifizierung geregelt; der Auftragnehmer selbst hat keinen physischen Zugang.
- Zugangskontrolle: Anmeldung an der Console nur mit persönlichem Konto; Passwörter werden ausschließlich als gesalzener scrypt-Hash gespeichert; Zwei-Faktor-Anmeldung wird angeboten; wiederholte Fehlversuche werden gebremst; Sitzungen laufen nach 30 Tagen ab und werden bei einer Passwortänderung beendet. Administrativer Zugang zu den Servern ist auf den Betreiber beschränkt und erfolgt ausschließlich verschlüsselt.
- Zugriffskontrolle: Rollenkonzept je Team (Inhaber, Admin, Entwickler, Leser); Zugriffsschlüssel für Schnittstellen lassen sich einzeln anlegen und widerrufen; Zugangsschlüssel zum Dateispeicher wahlweise nur mit Leserecht.
- Trennungskontrolle: Jede Anwendung läuft in einem eigenen Container mit festen Grenzen für Arbeitsspeicher, Rechenzeit und Prozesse, ohne Administratorrechte und ohne Zugriff auf andere Anwendungen. Datenbanken sind nur aus dem eigenen Netz des jeweiligen Teams erreichbar, nicht aus dem Internet.
- Weitergabekontrolle: Verbindungen zur Console, zur Schnittstelle und zu den Anwendungen werden per TLS (HTTPS) verschlüsselt. Anfragen an den Dateispeicher werden mit AWS Signature Version 4 signiert und nach 15 Minuten ungültig.
- Eingabekontrolle: Änderungen an Apps, Datenbanken, Speichern, Funktionen, Mitgliedern, Rollen und Abrechnungsdaten werden mit Person und Zeitpunkt im Protokoll des Teams festgehalten.
- Verfügbarkeitskontrolle: Tägliche Sicherung der Plattformdaten und der verwalteten Datenbanken; automatischer Neustart abgestürzter Anwendungen; minütliche Überwachung der Plattform mit Benachrichtigung des Betreibers bei Störungen und öffentlicher Statusseite.
- Wiederherstellbarkeit: Sicherungen werden aufbewahrt und lassen sich einzeln wiederherstellen; frühere Versionen einer App lassen sich mit einem Klick wieder in Betrieb nehmen.
- Überprüfung: Die Maßnahmen werden regelmäßig und bei jeder wesentlichen Änderung der Plattform überprüft; Sicherheitsupdates werden laufend eingespielt.

Anlage 2: Unterauftragsverarbeiter

Der Auftragnehmer setzt folgende Unterauftragsverarbeiter ein:

- Rechenzentrum und Server: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen. Standort der Server: Falkenstein (Vogtland), Deutschland. Leistung: Bereitstellung der Server, Stromversorgung, Netzanbindung und physische Sicherheit.