Allgemeine Geschäftsbedingungen für die Nutzung von

monatsabschluss.at

inkl. Bestimmungen zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Stand: September 2025

ihop it gmbh
Wallnerstraße 4/5/MT44
1010 Wien

1 Geltungsbereich

Diese AGB regeln die vertraglichen Bedingungen zwischen der ihop it gmbh (im Folgenden „Anbieter“) und den Nutzer*innen (im Folgenden „Kund*innen“), die die vom Anbieter bereitgestellte SaaS-App (Software as a Service Application) monatsabschluss.at zur Verwaltung und Aufbereitung von Ausgangs- und Eingangsrechnungen sowie damit verbundenen Dienstleistungen nutzen..

2 Leistungsbeschreibung

Die SaaS-App monatsabschluss.at ermöglicht Steuerberater*innen und deren Mandant*innen das Hochladen und Verarbeiten von Ausgangs- und Eingangsrechnungen sowie anderer Buchungsinformationen.

Die App bietet folgende Funktionen:

- Eigenregistrierung von Steuerberater*innen.
- Anlegen von Mandant*innen- und Benutzer*innenkonten durch Steuerberater*innen.
- Konfiguration der hochzuladenden Dateien (Buchungsinformationen, Helferdateien, AR-Belege) pro Mandant*in.
- Validierung der hochgeladenen Daten anhand von Kriterien die über einen Konfigurator von den Kund*innen definiert wurden.
- Erzeugung einer CSV-Datei mit Buchungszeilen, die anhand eines Konfigurators definiert wurden. Die Kriterien für die darin verwendeten mathematischen Formeln und Programmlogiken werden von den Kund*innen vorgegeben.
- Downloadfunktion für den Export der Buchungszeilen als CSV-Datei zur Einspielung in die Buchhaltungssoftware BMD als ZIP-Archiv zusammen mit allen für die Steuerberater*innen relevanten von den Mandant*innen bereitgestellten Dateien.

3 Datenspeicherung und -verarbeitung

Die Daten werden so lange aufbewahrt, wie dies zur Erfüllung der vertraglichen Leistungen notwendig ist, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Auf Anfrage können Kund*innen die Löschung ihrer Daten verlangen, soweit dies den gesetzlichen Vorgaben entspricht. Der Anbieter setzt geeignete technische und organisatorische Maßnahmen (TOMs) ein, um die Sicherheit der Daten zu gewährleisten.

4 Auftragsverarbeitung und Datenweitergabe an Dritte

Die Verarbeitung der personenbezogenen Daten der Kund*innen erfolgt im Rahmen der Nutzung der SaaS-App durch den Anbieter gemäß den Bestimmungen der DSGVO. Zur Bereitstellung der serverseitigen Infrastruktur wird die Digital Ocean LLC als Auftragsverarbeiter eingesetzt. Digital Ocean kann Subauftragsverarbeiter einsetzen, die ebenfalls den Vorgaben der DSGVO unterliegen. Die Daten werden auf Servern innerhalb der Europäischen Union gehostet. Die Vereinbarungen zur Auftragsverarbeitung zwischen der ihop it gmbh und Digital Ocean entsprechen den Vorgaben der DSGVO und können im Data Processing Agreement (DPA) von Digital Ocean eingesehen werden. (https://www.digitalocean.com/legal/data-processing-agreement).

5 Nutzung der App

Die Kund*innen sind verpflichtet, die App gemäß diesen AGB zu nutzen. Eine missbräuchliche Nutzung der App, insbesondere das Hochladen von unzulässigen, schadhaften oder urheberrechtlich geschützten Daten ohne Berechtigung, ist untersagt. Die App darf nur für den vorgesehenen Zweck der Buchhaltungsunterstützung und der Zusammenarbeit mit Steuerberater*innen verwendet werden.

6 Bereitstellung der Software und Infrastruktur

Die ihop it gmbh stellt den Kund*innen während der Vertragsdauer die SaaS-App sowie die notwendige serverseitige Infrastruktur als Dienstleistung zur Verfügung. Sämtliche Rechte an der SaaS-App und deren Inhalten verbleiben bei der ihop it gmbh. Die Kund*innen sind für die Bereitstellung und den Betrieb ihrer eigenen clientseitigen Infrastruktur (z.B. Endgeräte, Internetzugang, Software) selbst verantwortlich.

7 Service Level und Verfügbarkeit

Die ihop it gmbh stellt die SaaS-Anwendung auf einer „Best Effort"-Basis bereit und setzt alles daran, eine hohe Verfügbarkeit sicherzustellen. Die Verfügbarkeit der Anwendung ist jedoch abhängig von der Infrastruktur unseres Hosting-Anbieters Digital Ocean, auf deren Betrieb wir keinen direkten Einfluss haben. Eine uneingeschränkte Verfügbarkeit der SaaS-Anwendung kann daher nicht garantiert werden. Wir überwachen die Anwendung kontinuierlich und bieten im Falle von Störungen einen schnellen Support, um Unterbrechungen so gering wie möglich zu halten.

8 Support und Wartung

Der Anbieter bietet Support. Der Support für die Konfiguration von Mandat*innen ist kostenpflichtig. In bestimmten Paketen sind festgelegte Mengen an kostenfreiem Konfigurationssupport enthalten. Die Kund*innen können den Support über die im Vertrag festgelegten Kommunikationswege in Anspruch nehmen. Geplante Wartungsarbeiten werden den Kund*innen rechtzeitig mitgeteilt.

Der Support steht Mandant*innen werktags in der Zeit von 10-17 Uhr zur Verfügung. E-Mail Anfragen werden innerhalb von 24 Stunden beantwortet.

9 Haftung und Gewährleistung

Der Anbieter haftet nur für vorsätzliche oder grob fahrlässige Schäden. Für leichte Fahrlässigkeit haftet der Anbieter nur bei Verletzung wesentlicher Vertragspflichten (Kardinalpflichten). Der Anbieter haftet nur für vorsätzliche oder grob fahrlässige

Schäden. Für leichte Fahrlässigkeit haftet der Anbieter nur bei Verletzung wesentlicher Vertragspflichten (Kardinalpflichten). Eine Haftung für unvorhersehbare, indirekte und Folgeschäden sowie für Datenverlust oder falsche Prüfungen der hochgeladenen Dateien ist ausgeschlossen, soweit der Schaden nicht durch grobe Fahrlässigkeit des Anbieters verursacht wurde.

Der Anbieter übernimmt keine Haftung für Fehler, die durch fehlerhafte oder unvollständige Eingaben der Nutzer*innen entstehen.

10 Vertragslaufzeit und Kündigung

Die Vertragslaufzeit und Kündigungsmodalitäten ergeben sich aus den jeweils gültigen Entgeltbestimmungen.

11 Zahlungsbedingungen

Die Nutzung der SaaS-App erfolgt gegen Entgelt gemäß den jeweils gültigen Entgeltbestimmungen.
Abrechnung, Zahlungsmodalitäten, Rabatte sowie Verzugsregelungen ergeben sich ausschließlich aus den Entgeltbestimmungen.

12 Änderungen der AGB

Der Anbieter behält sich das Recht vor, diese AGB zu ändern. Änderungen werden den Kund*innen mindestens 30 Tage vor ihrem Inkrafttreten schriftlich oder per E-Mail mitgeteilt. Widersprechen die Kund*innen den Änderungen nicht innerhalb der Frist, gelten die neuen AGB als akzeptiert. Der Widerspruch bedarf der Schriftform.

13 Ausschluss fremder AGB

Es gelten ausschließlich die AGB der ihop it gmbh. Allgemeine Geschäftsbedingungen der Kund*innen, insbesondere Steuerberater*innen, finden keine Anwendung, auch wenn der Anbieter ihrer Geltung im Einzelfall nicht ausdrücklich widerspricht.

Abweichende Bedingungen der Kund*innen sind nur dann wirksam, wenn sie vom Anbieter ausdrücklich schriftlich anerkannt werden.

14 Gerichtsstand und anwendbares Recht

Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist Wien, Österreich. Es gilt das Recht der Republik Österreich unter Ausschluss des UN-Kaufrechts.

15 Bestimmungen zur Auftragsverarbeitung

15.1 Gegenstand, Dauer und Rangfolge

15.1.1 Gegenstand

Der Auftragsverarbeiter erbringt für den Verantwortlichen Dienstleistungen im Zusammenhang mit dem Betrieb und der Bereitstellung der SaaS-Plattform monatsabschluss.at (nachfolgend „Dienst“). Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag und auf dokumentierte Weisung des Verantwortlichen.

15.1.2 Dauer

Dieser AVV gilt für die Laufzeit des zwischen den Parteien bestehenden Hauptvertrags über die Nutzung des Dienstes („Hauptvertrag“) und endet automatisch mit dessen Beendigung. Regelungen zur Rückgabe/Löschung der Daten gelten über das Vertragsende hinaus, soweit erforderlich.

15.1.3 Rangfolge

Bei Widersprüchen zwischen AVV und Hauptvertrag gehen die Bestimmungen dieses AVV den datenschutzbezogenen Bestimmungen des Hauptvertrags vor. Im Übrigen gilt der Hauptvertrag vorrangig.

15.2 Art und Zweck der Verarbeitung - Kategorien betroffener Personen und Daten

15.2.1 Zweck

Verarbeitung zur Erbringung des Dienstes monatsabschluss.at, insbesondere: Entgegennahme strukturierter Dateien (z. B. CSV/JSON/XLSX/XML/PDF) zu Aus- und Eingangsrechnungen und sonstiger Dateien, Validierung und Aufbereitung, Erzeugung von Exportdateien (z. B. BMD-CSV) sowie begleitende Support-, Wartungs- und Sicherheitsleistungen.

15.2.2 Arten der Verarbeitung

Erheben (durch Upload), Speichern, Ordnen, Strukturieren, Anpassen/Ändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung (z. B. an den Verantwortlichen), Abgleichen, Einschränken, Löschen/Vernichten, Protokollieren.

15.2.3 Betroffene Personengruppen (Beispiele)

Mandant:innen des Verantwortlichen (Kunden von Steuerberatungskanzleien), deren Kunden/Kontaktpersonen, Lieferanten/Business-Partner, ggf. Mitarbeiter:innen der Mandant:innen (sofern in Dateien enthalten), Kontaktpersonen des Verantwortlichen.

15.2.4 Datenkategorien (Beispiele, je nach Konfiguration)

Stammdaten (Name/Firma, Adresse, UID, Kundennummer), Kontaktdaten (E-Mail, Telefon), Rechnungs-/Buchungsdaten (Rechnungsnummer, Datum, Beträge, Steuersätze, Konto/Kostenstelle, Leistungs-/Lieferzeitraum), Zahlungsinformationen (z. B. IBAN in Rechnungen), Vertrags-/Belegmetadaten, Protokolldaten (z. B. IP, Zeitstempel) aus Sicherheits- und Fehlerlogs.

15.2.5 Besondere Kategorien

Die Verarbeitung besonderer Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO ist nicht beabsichtigt. Sollte der Verantwortliche solche Daten in den Dienst einspielen, hat er dies ausdrücklich anzuweisen und die rechtlichen Voraussetzungen zu schaffen.

15.3 Rechte und Pflichten des Verantwortlichen

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, die Information der Betroffenen, die Wahrnehmung ihrer Rechte sowie für die Qualität und Rechtmäßigkeit der an den Auftragsverarbeiter übermittelten Daten verantwortlich. Er dokumentiert seine Weisungen (z. B. im Vertrag, über das Admin-Interface, Tickets oder E-Mail) und teilt Änderungen rechtzeitig mit.

15.4 Pflichten des Auftragsverarbeiters

15.4.1 Verarbeitung nur auf Weisung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern nicht eine unions- oder mitgliedstaatliche Rechtsvorschrift ihn hierzu verpflichtet. In diesem Fall informiert er den Verantwortlichen vor der Verarbeitung, sofern die Rechtsvorschrift eine solche Information nicht wegen eines wichtigen öffentlichen Interesses verbietet.

15.4.2 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass zur Verarbeitung befugte Personen (Mitarbeiter:innen, Erfüllungsgehilfen) zur Vertraulichkeit verpflichtet wurden und eine angemessene Schulung erhalten.

15.4.3 Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen TOM nach Art. 32 DSGVO und hält diese auf einem dem Risiko angemessenen Stand. Wesentliche Änderungen, die die Sicherheit wesentlich beeinträchtigen könnten, bedürfen der vorherigen Zustimmung des Verantwortlichen.

15.4.4 Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen (unter Berücksichtigung der Art der Verarbeitung) bei der Erfüllung von Betroffenenrechten (Art. 12–23 DSGVO), bei Meldungen von Verletzungen des Schutzes personenbezogener Daten (Art. 33, 34

DSGVO), bei Datenschutz-Folgenabschätzungen einschließlich vorheriger Konsultation (Art. 35, 36 DSGVO) sowie bei der Einhaltung der Sicherheit der Verarbeitung (Art. 32 DSGVO).

15.4.5 Meldung von Datenschutzvorfällen

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich und ohne unangemessene Verzögerung nach Kenntniserlangung von einer Verletzung des Schutzes personenbezogener Daten. Die Meldung enthält nach Möglichkeit die in Art. 33 Abs. 3 DSGVO genannten Informationen.

15.4.6 Löschung und Rückgabe

Nach Abschluss der vertraglichen Leistungen oder auf Weisung des Verantwortlichen wird der Auftragsverarbeiter sämtliche personenbezogenen Daten zurückgeben oder löschen; Ausnahmen bestehen, soweit eine gesetzliche Aufbewahrungspflicht besteht. Details siehe Anlage 4.

15.4.7 Nachweise und Audits

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem AVV festgelegten Pflichten zur Verfügung und ermöglicht Audits – einschließlich Inspektionen – durch den Verantwortlichen oder einen von ihm beauftragten Prüfer, jeweils mit angemessener vorheriger Ankündigung, zu üblichen Geschäftszeiten und unter Wahrung der Vertraulichkeit. Der Auftragsverarbeiter kann den Nachweis auch durch geeignete Zertifikate, Prüfberichte, Policies oder Sicherheitskonzepte erbringen. Ein Audit pro Kalenderjahr ist kostenfrei, darüber hinausgehende oder anlassbezogene Audits können nach angemessenem Aufwand vergütet werden.

15.5 Unterauftragsverhältnisse

15.5.1 Genehmigung

Der Verantwortliche erteilt hiermit die allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern (Sub-Prozessoren). Der Auftragsverarbeiter verpflichtet jeden Sub-Prozessor vertraglich auf mindestens das Schutzniveau dieses AVV.

15.5.2 Information/Opt-out

Der Auftragsverarbeiter informiert den Verantwortlichen vorab über beabsichtigte Änderungen in der Liste der Sub-Prozessoren (siehe Anlage 3). Der Verantwortliche kann aus wichtigem Grund innerhalb von 14 Tagen widersprechen; die Parteien suchen in diesem Fall nach einer einvernehmlichen Lösung.

15.5.3 Verantwortlichkeit

Der Auftragsverarbeiter bleibt für die Pflichten der Sub-Prozessoren gegenüber dem Verantwortlichen verantwortlich.

15.6 Internationale Datenübermittlungen

Eine Übermittlung personenbezogener Daten in Drittländer außerhalb des EWR erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss, Abschluss der EU-Standardvertragsklauseln einschließlich Durchführung einer Transfer Impact Assessment und ggf. ergänzender Maßnahmen). Details und betroffene Sub-Prozessoren sind in Anlage 3 zu dokumentieren.

15.7 Vergütung

Soweit in diesem AVV nichts Abweichendes geregelt ist, sind die Leistungen des Auftragsverarbeiters durch die Entgelte des Hauptvertrags abgegolten. Zusatzleistungen (z. B. außergewöhnlicher Support/Audit-Begleitung) werden nach den im Hauptvertrag vereinbarten Sätzen oder – mangels Regelung – nach angemessenem Aufwand abgerechnet.

15.8 Geheimhaltung und Schutz von Geschäftsgeheimnissen

Die Parteien wahren Vertraulichkeit über alle im Rahmen dieses AVV erlangten Informationen. Etwaige weitergehende Vertraulichkeitsvereinbarungen bleiben unberührt.

15.9 Schlussbestimmungen

15.9.1 Schriftform

Änderungen und Ergänzungen dieses AVV bedürfen der Textform und einer eindeutigen Bezugnahme auf diesen Vertrag.

15.9.2 Anwendbares Recht und Gerichtsstand

Es gilt österreichisches Recht unter Ausschluss dessen Kollisionsnormen. Ausschließlicher Gerichtsstand ist – soweit zulässig – Wien. Zwingende Verbraucherregelungen bleiben unberührt (nicht einschlägig bei B2B-Verhältnis).

15.9.3 Salvatorische Klausel

Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame Bestimmung durch eine wirksame ersetzen, die ihrem wirtschaftlichen Zweck am nächsten kommt.

Anlage 1: Beschreibung der Verarbeitung

Dienst/Produkt: monatsabschluss.at (SaaS)

Verarbeitungszwecke: Upload, Validierung und Aufbereitung buchhaltungsrelevanter Dateien; Generierung von Exportdateien (z. B. BMD-CSV); Bereitstellung für den Verantwortlichen; Support und Qualitätssicherung.

Kategorien betroffener Personen: siehe Ziff. 2.3.

Datenkategorien: siehe Ziff. 2.4 (konkret je Mandant/Projekt auszufüllen).

Verarbeitungsort: primär EU/EWR (Details in Anlage 3).

Speicherdauer: gemäß Weisung des Verantwortlichen und gesetzlicher Pflichten; Standardfristen siehe Anlage 4.

Anlage 2: Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

Die folgenden Maßnahmen stellen den zum Zeitpunkt des Vertragsschlusses implementierten Standard dar. Der Auftragsverarbeiter hält ein internes Sicherheitskonzept vor und überprüft/aktualisiert die Maßnahmen regelmäßig.

A. Vertraulichkeit (Zutritts-/Zugangs-/Zugriffskontrolle)

- Rechenzentrums-Sicherheit gemäß branchenüblichen Standards (physische Zutrittskontrollen beim IaaS-Provider; Protokollierung).

- Rollenbasierte Berechtigungen (Least Privilege).

- Netzwerksegmentierung, Firewalls, abgesicherte Management-Schnittstellen; VPN für Administrationszugriffe.

- Verschlüsselung in Transit (TLS ≥ 1.2) und at Rest (z. B. verschlüsselte Volumes/DB-Funktionen), Schlüsselverwaltung mit restriktivem Zugriff.

- Geheimnis-/Schlüssel-Management (z. B. .env-Secrets im Secret-Store, kein Hardcoding).

- Protokollierung von administrativen Aktionen; Schutz vor unberechtigten Exporten (Download-/API-Kontrollen).

B. Integrität (Weitergabe- und Eingabekontrolle)

- Signierte Deployments, Vier-Augen-Prinzip bei produktiven Änderungen; CI/CD-Freigabeprozesse.

- Prüfsummen/Hash-Verfahren bei Dateiübernahmen; Versionierung und Nachvollziehbarkeit von Änderungen.

- Rechte-/Rollenprüfung vor Export/Download/API-Zugriffen.

C. Verfügbarkeit und Belastbarkeit

- Regelmäßige Backups der produktiven Datenbanken und Upload-Dateien; getestete Restore-Prozesse (mind. jährlich).

- Monitoring und Alerting (z. B. System-/Applikations-/Sicherheitslogs); DDoS-/Ressourcen-Schutz auf Infrastruktur-Ebene.

- Patching-/Vulnerability-Management (inkl. Sicherheitsupdates mit Priorisierung).

- Notfall- und Incident-Prozess inkl. Kommunikationsplan.

D. Pseudonymisierung/Datensparsamkeit

- Trennung von Produktiv- und Testdaten; keine produktiven personenbezogenen Daten in Tests ohne Anonymisierung.

- Konfigurierbare Datenaufbewahrung; automatische Löschroutinen nach Weisung.

E. Organisation/Compliance

- Vertraulichkeitsverpflichtungen und Datenschutz-Schulungen für Mitarbeitende.

- Berechtigungskonzepte und regelmäßige Reviews (mind. jährlich).

- Need-to-know-Prinzip bei Supportzugriffen (zeitlich begrenzte, dokumentierte Freigaben).

- Datenschutz-Folgenabschätzung-Unterstützung auf Anfrage; Change-/Risk-Management.

- Auftrags- und Sub-Prozessor-Management mit Dokumentation.

Anlage 3: Liste der Unterauftragsverarbeiter (Sub-Prozessoren)

Der Auftragsverarbeiter informiert den Verantwortlichen vor Änderungen. Nachfolgende Tabelle ist beim Onboarding zu befüllen.

Anbieter	Leistung	Verarbeitungsort	Drittland-bezug	Rechts-instrument
DigitalOcean, LLC	IaaS/Hosting der Produktiv-Systeme	EU-Rechenzentrum (z. B. Frankfurt/ Amsterdam)	USA (konzern-bedingt)	EU-SCC + TIA, ergänzende Maßnahmen
Microsoft 365 (Exchange Online)	E-Mail-Kommunikation/ Support-Tickets (sofern personenbezogene Daten enthalten)	EU/EWR (gem. Anbieterangaben)	ggf. USA (konzern-bedingt)	EU-SCC + TIA

Anlage 4: Datenrückgabe, Löschung und Aufbewahrung

- Rückgabeformat: maschinenlesbar (z. B. CSV/ZIP/PDF) über das Portal oder gesichert per Übertragung auf Weisung.

- Standard-Löschfristen:

• Mandanten-Uploads (Dateien): Daten werden nach Ablauf der vereinbarten Speicherdauer gelöscht, Details siehe Entgeltbestimmungen.

• Metadaten/Protokolle: 180 Tage (Sicherheits-/Fehlerlogs).

• Backups: automatische Überschreibung nach 14 Tagen (Rolling Backup).

- Sperrung statt Löschung, sofern gesetzliche Aufbewahrungspflichten entgegenstehen; Löschung unverzüglich nach Wegfall dieser Pflichten.

- Nachweis: Der Auftragsverarbeiter dokumentiert die Löschung auf Anfrage (z. B. Löschprotokoll/Bestätigung).