SLA

SERVICE LEVEL AGREEMENT

Service Level Agreement

für die Nutzung der faktoora SaaS-Plattform

DSGVO · GoBD · ISMS ausgerichtet an ISO/IEC 27001:2022 · gültig ab 01.12.2026

VERSION	GÜLTIGKEIT	LETZTES REVIEW	VERANTWORTLICH
4.2	01.12.2026	29.10.2026	faktoora GmbH – Geschäftsführung

Inhaltsverzeichnis

Hinweis: Diese Fassung gilt ab dem 01.12.2026. Bis zum 30.11.2026 gilt die bisherige Fassung: SLA Version 4.1 (PDF).

01	Einleitung und Zweck	03
02	Geltungsbereich	04
03	Begriffsbestimmungen	05
04	Verfügbarkeit der Plattform	06
05	Supportleistungen	08
06	Datensicherheit und Verschlüsselung	09
07	Zertifizierungen und Compliance	11
08	Zugriffskontrolle und Audit-Logging	12
09	Change Management und Wartung	13
10	Sicherheitsvorfälle – Incident Management	14
11	Datenschutz und Datenlokalisierung	16
12	Audit-Rechte und Nachweispflichten	17
13	Business Continuity und Disaster Recovery	18
14	Reporting und Transparenz	19
15	Gültigkeit, Änderungen und Sonderkündigungsrecht	20
16	Anerkennung	21

Einleitung und Zweck

Dieses Service Level Agreement (SLA) der faktoora GmbH regelt die Service Level der faktoora SaaS-Plattform und beschreibt Sicherheit, Betriebskontinuität und Supportbetrieb. Es ergänzt den Hauptvertrag sowie den Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO.

Verbindliche Leistungszusagen enthalten die Abschnitte 4, 5 und 10.1. Die übrigen Abschnitte beschreiben den derzeitigen Stand der Maßnahmen; faktoora kann sie entsprechend Ziffer 4 Abs. 2 AVV anpassen, sofern das Schutzniveau nicht unterschritten wird. Verbindlich für die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO ist Anlage 2 der AVV. Garantien im Sinne von Ziffer 9.2 der AGB übernimmt faktoora mit diesem SLA nicht.

Das Dokument orientiert sich an den Anforderungen folgender Standards:

- ISO/IEC 27001:2022 – Informationssicherheits-Managementsystem (ISMS ausgerichtet an der Norm)
- DSGVO – Datenschutz-Grundverordnung
- GoBD – Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff

Das SLA gilt für Kunden mit dem Tarif „Enterprise“ (bisher „Individuell“) und aktivem Vertrag. Kunden mit einem anderen kostenpflichtigen Tarif, deren Vertrag vor dem 01.12.2026 geschlossen wurde, behalten das SLA für die Dauer dieses Vertrags (Bestandsschutz). Für andere Tarife und kostenfreie Testzugänge findet es keine Anwendung, sofern nicht ausdrücklich in Textform vereinbart.

Diese Fassung gilt ab dem 01.12.2026. Für Kunden, deren Vertrag vor diesem Tag geschlossen wurde, gilt sie ab dem 01.12.2026, frühestens jedoch vier Wochen nach Zugang der Änderungsmitteilung, sofern der Kunde nicht nach Ziffer 8.10 der AGB widerspricht; bis dahin gilt die bisherige Fassung.

Geltungsbereich

Dieses SLA gilt für alle Dienste und Komponenten, die faktoora direkt betreibt, insbesondere:

- SaaS-Plattform faktoora (Webanwendung und API)
- Authentifizierungs- und Autorisierungsinfrastruktur
- Datenspeicherung und Datenbankbetrieb
- Backup- und Wiederherstellungsinfrastruktur
- Supportleistungen gemäß Abschnitt 5

Ausdrücklich nicht erfasst: Dienste von Drittanbietern (externe Payment Provider, E-Mail-Dienstleister, Netzwerkinfrastruktur von Internet Service Providern, Endgeräte des Kunden).

Begriffsbestimmungen

BEGRIFF	DEFINITION
Verfügbarkeit	Prozentualer Anteil eines Kalendermonats ohne Downtime.
Downtime	Zeitraum, in dem Webanwendung und API am Routerausgang des Rechenzentrums (Ziffer 2.2 AGB) nicht erreichbar sind, festgestellt durch die Überwachung von faktoora; ausgenommen sind geplante Wartung und die Ausschlüsse nach Abschnitt 4.3.
Geplante Wartung	Wartung innerhalb der festen Wartungsfenster sowie angekündigte größere Wartung im Rahmen von Abschnitt 9.1, während der die Plattform eingeschränkt oder nicht verfügbar sein kann.
Reaktionszeit	Zeit zwischen Eingang einer Meldung und erster qualifizierter Rückmeldung durch faktoora.
RTO (Recovery Time Objective)	Angestrebte Zeitspanne vom Ausfall bis zur Wiederherstellung der Betriebsbereitschaft, gerechnet innerhalb der Geschäftszeiten (Zielwert).
RPO (Recovery Point Objective)	Angestrebter maximaler Datenverlust-Zeitraum im Notfall (Zielwert).
Incident	Sicherheitsvorfall oder Störung, die Verfügbarkeit oder Datensicherheit beeinträchtigt.
SLA-Credit	Geldwerte Gutschrift auf die Monatsgebühr als Kompensation bei SLA-Verletzung.
Change	Änderung an Systemkomponenten, Konfigurationen oder Softwareversionen.
ISMS	Informationssicherheits-Managementsystem, ausgerichtet an ISO/IEC 27001:2022.
Audit-Log	Manipulationserkennbare Aufzeichnung aller sicherheitsrelevanten Ereignisse und Zugriffe (append-only, kryptografische Hash-Kette).

Verfügbarkeit der Plattform

4.1 Verfügbarkeitszusage

faktoora sagt im Geltungsbereich dieses SLA eine monatliche Mindest-Verfügbarkeit von 99,5 % zu.

SERVICE-TIER	VERFÜGBARKEIT/MONAT	MAX. DOWNTIME/MONAT	MAX. DOWNTIME/JAHR
Tarif „Enterprise“ und Bestandskunden (Ziffer 01)	99,5 %	ca. 3,6 Stunden	ca. 43,8 Stunden

Die Verfügbarkeitszusage bezieht sich auf die Zeit außerhalb der festen Wartungsfenster nach Abschnitt 9.1 (Mo–Fr 18:00–22:00 Uhr und samstags ganztägig). Zeiten in diesen Wartungsfenstern sowie angekündigte größere Wartung nach Abschnitt 9.1 bis zu insgesamt 8 Stunden je Kalendermonat gehen nicht in die Berechnung der Verfügbarkeit ein.

Messmethodik

Grundlage der Verfügbarkeitsberechnung ist die interne Störungsdokumentation von faktoora; der Kunde kann der Berechnung unter Vorlage eigener Aufzeichnungen widersprechen. Messzeitraum ist der Kalendermonat. Geplante Wartung im Rahmen von Abschnitt 9.1 wird nicht als Downtime gezählt. Kunden können jederzeit eine Statusabfrage per E-Mail anfordern; eine Übersicht der dokumentierten Störungen ist auf Anfrage erhältlich. Die Plattform wird automatisiert überwacht.

4.2 SLA-Credits bei Nichteinhaltung

Bei Unterschreitung der zugesagten Verfügbarkeit hat der Kunde Anspruch auf folgende Gutschriften:

TATSÄCHLICHE VERFÜGBARKEIT	SLA-CREDIT
99,0 % bis < 99,5 %	5 % der Monatsgebühr
95,0 % bis < 99,0 %	10 % der Monatsgebühr
< 95,0 %	25 % der Monatsgebühr

Credits müssen innerhalb von 30 Tagen nach dem betreffenden Monat in Textform bei support@faktoora.com beantragt werden. Sie sind auf die Monatsgebühr des betreffenden Zeitraums begrenzt; bei jährlicher Abrechnung gilt ein Zwölftel der Jahresgebühr als Monatsgebühr. Mit den SLA-Credits sind Minderungsansprüche wegen der Unterschreitung der Verfügbarkeit abgegolten. Die Überschreitung von Reaktionszeiten (Abschnitt 5.2) löst keine SLA-Credits aus. SLA-Credits werden auf etwaige Schadensersatzansprüche angerechnet; im Übrigen gilt die Haftungsregelung der AGB (Ziffer 9).

4.3 Ausschlüsse

Folgende Zeiträume zählen nicht als Downtime:

- Wartung in den festen Wartungsfenstern nach Abschnitt 9.1

- Angekündigte größere Wartung außerhalb der festen Wartungsfenster nach Abschnitt 9.1, bis zu insgesamt 8 Stunden je Kalendermonat
- Höhere Gewalt (Naturkatastrophen, Streik, staatliche Eingriffe)
- Ausfälle, die durch den Kunden oder durch Dritte verursacht wurden, die nicht Erfüllungsgehilfen von faktoora sind
- Netzwerkausfälle bei Internet Service Providern
- DDoS-Angriffe, die die Schutzmechanismen des Hosting-Anbieters überschreiten

Supportleistungen

5.1 Kontakt und Geschäftszeiten

KANAL	ADRESSE / NUMMER	VERFÜGBARKEIT
E-Mail (Standard)	support@faktoora.com	24/7 Eingang; Bearbeitung Mo–Fr 09–17 Uhr (MEZ/MESZ)
Telefon (nur Tarif „Enterprise“)	+49 731 85070390	Mo–Fr, 09:00–17:00 Uhr (MEZ/MESZ)
Sicherheitsvorfälle	security@faktoora.com	24/7 Eingang; priorisierte Bearbeitung gemäß Abschnitt 10

Geschäftszeiten: Montag bis Freitag, 09:00–17:00 Uhr (MEZ/MESZ), ausgenommen gesetzliche Feiertage in Bayern.

5.2 Prioritäten und Reaktionszeiten

PRIO	BESCHREIBUNG	REAKTIONSZEIT
A – Kritisch	Plattform vollständig ausgefallen oder Datenverlust. Kein Workaround.	1 Stunde
B – Hoch	Wesentliche Funktion beeinträchtigt, Workaround möglich.	4 Stunden
C – Mittel	Funktionseinschränkung ohne kritische Auswirkung.	1 Geschäftstag
D – Gering	Kosmetische Fehler, Verbesserungswünsche, allgemeine Anfragen.	2 Geschäftstage

Die Reaktionszeiten gelten innerhalb der Geschäftszeiten (Mo–Fr 09:00–17:00 Uhr MEZ/MESZ). Außerhalb der Geschäftszeiten beginnen die Fristen mit dem nächsten Geschäftstag. Prio A: Kritische Incidents werden durch automatisiertes Monitoring erkannt und soweit möglich automatisch behandelt; die menschliche Reaktion erfolgt innerhalb von 1 Stunde ab Beginn der nächsten Geschäftszeiten. Lösungszeiten werden nicht zugesagt; faktoora bearbeitet Störungen nach ihrer Priorität.

5.3 Eskalationsverfahren

Der Kunde kann eine Meldung jederzeit per E-Mail mit dem Betreff "ESKALATION: [Ticket-ID]" eskalieren; faktoora prüft dann die Priorisierung und informiert den Kunden über das weitere Vorgehen.

Datensicherheit und Verschlüsselung

Die nachfolgenden Angaben beschreiben den derzeitigen Stand der Maßnahmen; verbindlich für die technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 DSGVO ist Anlage 2 der AVV.

6.1 Verschlüsselung

BEREICH	STANDARD	DETAILS
Daten at rest	Festplattenvollverschlüsselung	Vollverschlüsselung aller Produktionssysteme. Schlüsselverwaltung über dokumentierte Verfahren mit beschränktem Personenkreis.
Daten in transit	TLS 1.2 oder höher	Ausschließlich sichere Protokolle für alle externen Verbindungen.
Backups	Verschlüsselte Backups	Backups werden verschlüsselt übertragen und an einem räumlich getrennten Standort gespeichert.
Zugangsdaten	Selbst betriebener Identity Provider; alternativ Single Sign-on über den Identity Provider des Kunden	Passwörter werden ausschließlich gehasht beim Identity Provider verwaltet; die Anwendung selbst speichert keine Passwörter. Bei Single Sign-on (z. B. Microsoft Entra ID) erfolgt die Anmeldung beim Identity Provider des Kunden. API-Schlüssel werden nur als Hash abgelegt.

6.2 Backup und Wiederherstellung

PARAMETER	WERT
Backup-Frequenz	Sicherung aller persistenten Datenbestände (Datenbanken, Dateispeicher, Audit-Logs) mindestens alle 2 Stunden; zusätzlich tägliche vollständige System-Snapshots
Aufbewahrungszeit	14 Tage (Tages-Backups); bis zu 12 Monate (Monats-Backups)
RPO (Recovery Point Obj.)	Zielwert: 2 Stunden
RTO (Recovery Time Obj.)	Zielwert: 8 Stunden innerhalb der Geschäftszeiten für die vollständige Plattform-Wiederherstellung; einzelne Dienste typischerweise deutlich schneller
Backup-Standort	ISO 27001-zertifizierte Rechenzentren in Deutschland (Hetzner), räumlich getrennt von der Produktion
Backup-Tests	Regelmäßige dokumentierte Wiederherstellungsübungen
Integritätsprüfung	Prüfsummengesicherte Backups mit regelmäßiger Integritätsprüfung

6.3 Ausfallsicherheit und Wiederherstellung

- Container-Plattform mit automatischem Neustart ausgefallener Dienste
- Dokumentiertes Verfahren zur Wiederherstellung der Gesamtplattform aus einem System-Snapshot auf neuer Infrastruktur
- Zwei unabhängige Backup-Ebenen (verschlüsselte Daten-Backups und tägliche System-Snapshots)

- Hosting in ISO 27001-zertifizierten Rechenzentren mit redundanter Strom- und Netzwerkversorgung

Zertifizierungen und Compliance

7.1 Zertifizierungen und Standards

ZERTIFIZIERUNG / STANDARD	SCOPE	STATUS	NACHWEIS
ISO/IEC 27001:2022	ISMS der faktoora SaaS-Plattform	ISMS ausgerichtet an ISO/IEC 27001:2022	Statement of Applicability (Zusammenfassung) auf Anfrage
ISO 27001 – RZ	Hosting-Infrastruktur	Zertifiziert	RZ-Zertifikat auf Anfrage
DSGVO / Art. 28	Auftragsverarbeitung	AVV nach Art. 28 DSGVO	AVV als Vertragsbestandteil
GoBD	Speicherung von Rechnungen während der Vertragslaufzeit	Manipulationserkennbarer Audit-Trail; Schutz vor Löschung während der Vertragslaufzeit; die gesetzliche Aufbewahrung obliegt dem Kunden	Beschreibung der Speicherung und des Exports auf Anfrage

faktoora stellt auf Anfrage verfügbare Zertifikate und Nachweise bereit. Prüfberichte unabhängiger Stellen werden, soweit vorhanden, auf Anfrage und nach Unterzeichnung einer NDA zur Verfügung gestellt.

7.2 GoBD-Konformität

- Manipulationserkennbarer Audit-Trail (append-only, kryptografische Hash-Kette)
- Protokollierung aller über die Anwendung vorgenommenen geschäftsrelevanten Änderungen mit Zeitstempel und Benutzeridentifikation
- Datenexport per Self-Service als CSV und PDF, für einzelne Datenbereiche auch als XLSX; ergänzend auf Anfrage als JSON
- Manipulationserkennbare Speicherung während der Vertragslaufzeit und vollständiger Export nach Ziffer 5.2 AGB; die gesetzliche Aufbewahrung (8 Jahre für Rechnungen und Buchungsbelege, 10 Jahre für Bücher und Aufzeichnungen, § 147 AO) obliegt dem Kunden

Zugriffskontrolle und Audit-Logging

8.1 Zugriffskontrolle

- Rollenbasiertes Zugriffsmodell (RBAC) nach Least-Privilege-Prinzip
- Mehrfaktorauthentifizierung für administrative Infrastrukturzugänge (Server-, Cloud- und Entwicklungszugänge)
- Regelmäßige Überprüfung der Produktions- und Entwicklerzugriffsrechte
- Unverzügliche Zugangssperrung beim Ausscheiden von Mitarbeitern
- Zugriff auf die Produktionsumgebung ist auf einen kleinen, namentlich benannten Personenkreis beschränkt
- Strikte Trennung von Entwicklungs-, Test- und Produktionsumgebung; keine automatisierten CI/CD-Zugriffe auf die Produktion

8.2 Audit-Logging

- Protokollierung von Authentifizierungsereignissen
- Protokollierung administrativer Änderungen in der Anwendung im Audit-Trail sowie aller Anmeldungen an Produktionssystemen
- Append-only Audit-Trail mit kryptografischer Hash-Kette; Manipulationen sind technisch erkennbar
- Aufbewahrung anwendungsbezogener Audit-Logs während der Vertragslaufzeit; nach Vertragsende gilt Ziffer 12 AVV
- Auskunft über protokollierte eigene Daten im Rahmen der DSGVO-Betroffenenrechte

Change Management und Wartung

Änderungen unterliegen einem formalen Change-Management-Prozess mit automatisierten Qualitätsprüfungen und Rollback-Fähigkeit.

9.1 Wartungsfenster

ART	ZEITFENSTER	ANKÜNDIGUNG
Regelmäßige Wartung	Feste Wartungsfenster Mo–Fr 18:00–22:00 Uhr und samstags ganztägig (MEZ/MESZ)	Keine gesonderte Ankündigung
Größere Wartung außerhalb der festen Wartungsfenster	Nach Bedarf, vorzugsweise außerhalb der Geschäftszeiten; bis zu insgesamt 8 Stunden je Kalendermonat nicht als Downtime gezählt, darüber hinaus als Downtime	Mindestens 48 Stunden vorab per E-Mail

9.2 Notfall-Changes

- Kritische Sicherheits-Patches können ohne Vorankündigung eingespielt werden
- Information betroffener Kunden zeitnah, soweit die Änderung Auswirkungen auf sie hat
- Incident-Report auf Anfrage verfügbar

Sicherheitsvorfälle – Incident Management

10.1 Klassifikation und Meldepflichten

SCHWEREGRAD	BESCHREIBUNG	INTERNE REAKTION (ZIELWERT)	KUNDENMELDUNG	BEHÖRDENMELDUNG
P1 – Kritisch	Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO), insbesondere Verlust, unbefugte Offenlegung oder unbefugter Zugang	Automatisierte Überwachung; Bewertung unverzüglich während der Geschäftszeiten, außerhalb der Geschäftszeiten ab Beginn des nächsten Geschäftstags	unverzüglich, spätestens innerhalb von 4 Stunden nach Einstufung als kritisch	Meldung an die Aufsichtsbehörde durch den Kunden als Verantwortlichen (Art. 33 DSGVO); faktoora unterstützt gemäß Ziffer 9 AVV
P2 – Hoch	Systemkompromittierung ohne bestätigten Datenverlust	Unverzüglich (Geschäftszeiten)	Unverzüglich (Geschäftszeiten), soweit Kunden betroffen sind	Durch den Kunden als Verantwortlichen, soweit erforderlich
P3 – Mittel	Anomalie mit möglichen Sicherheitsauswirkungen	1 Geschäftstag	Auf Anfrage	I. d. R. nicht nötig
P4 – Gering	Potenzielle Schwachstelle ohne aktive Ausnutzung	5 Geschäftstage	Auf Anfrage	Nicht erforderlich

Die Meldepflichten nach Ziffer 9 AVV bleiben unberührt; Meldungen an Aufsichtsbehörden zu Daten, die faktoora im Auftrag verarbeitet, erfolgen durch den Kunden.

10.2 Incident-Response-Prozess

- Erkennung: Identifikation über Monitoring, Alerts oder Kundenmeldung
- Eindämmung: Sofortige Schadensbegrenzung (Isolation, Zugangssperrung)
- Analyse: Root Cause Analysis und Auswirkungsbewertung
- Behebung: Implementierung der Korrekturmaßnahmen und Wiederherstellung
- Abschlussbericht: Interner Post-Incident-Review; zusammenfassender Bericht an betroffene Kunden auf Anfrage
- Lessons Learned: Erkenntnisse fließen in ISMS und Prozessdokumentation ein

10.3 Schwachstellenmanagement

- Automatisierte Schwachstellen-Scans in der CI-Pipeline (Scanning der Abhängigkeiten auf bekannte Schwachstellen und statische Code-Analyse)
- Regelmäßige Penetrationstests sind in unserem Testprogramm festgelegt
- Risikobasierte, priorisierte Behebung: kritische Schwachstellen werden unverzüglich behandelt

- Ergebnisse durchgeführter Penetrationstests stellen wir auf Anfrage (unter NDA) zusammengefasst bereit

Datenschutz und Datenlokalisierung

- Hosting und Speicherung der Plattformdaten erfolgen in ISO 27001-zertifizierten Rechenzentren in Deutschland; einzelne Unterauftragnehmer verarbeiten Daten für ihre jeweilige Leistung auch an anderen Orten (Anlage 3 des AVV und trust.faktoora.com)
- Übermittlungen in Drittländer und die jeweiligen Garantien nach Art. 44 ff. DSGVO sind in Anlage 3 des AVV aufgeführt
- Auftragsverarbeitung geregelt im AVV gemäß Art. 28 DSGVO
- Betroffenenanfragen (Art. 15–22 DSGVO) zu Kundendaten leitet faktoora unverzüglich an den Kunden weiter und unterstützt ihn nach Ziffer 5 AVV
- Externer Datenschutzbeauftragter: PROLIANCE GmbH, datenschutzbeauftragter@datenschutzexperte.de

Audit-Rechte und Nachweispflichten

- Es gelten die Kontrollrechte nach Ziffer 8 AVV; bei Widersprüchen geht die AVV vor
- faktoora stellt auf Anfrage (unter NDA) geeignete Nachweise nach eigener Wahl bereit
- Die Bereitstellung vorhandener Nachweise und Auskünfte ist unentgeltlich; für Inspektionen sowie individuelle Prüfungen und Fragebögen gilt Ziffer 8 Abs. 4 AVV

Business Continuity und Disaster Recovery

faktoora betreibt ein Business-Continuity- und Disaster-Recovery-Management.

PARAMETER	ZIELWERT
RTO – Gesamtplattform	Zielwert: 8 Stunden innerhalb der Geschäftszeiten
RTO – Einzelne Dienste	Typischerweise unter 1 Stunde (automatische Wiederherstellung)
RPO	Zielwert: 2 Stunden
DR-Tests	Regelmäßig, dokumentiert
BCP-Review	Regelmäßig sowie nach wesentlichen Systemänderungen
Backup-Ebenen	Zwei unabhängige Backup-Ebenen (verschlüsselte Daten-Backups und tägliche System-Snapshots)

Reporting und Transparenz

- Übersicht der dokumentierten Störungen und Wartungszeiten auf Anfrage
- Benachrichtigung betroffener Kunden bei Incidents per E-Mail gemäß Abschnitt 10

Gültigkeit, Änderungen und Sonderkündigungsrecht

- Dieses SLA gilt für die Dauer des zugrundeliegenden Hauptvertragsverhältnisses
- faktoora überprüft das SLA regelmäßig
- Änderungen werden mindestens vier Wochen vor Inkrafttreten in Textform mitgeteilt; im Übrigen gilt Ziffer 8.10 der AGB entsprechend (Widerspruch, Kündigung des Hauptvertrags bis zum Wirksamwerden der Änderung)
- Das jeweils aktuelle SLA ist unter faktoora.com/dokumente abrufbar

Anerkennung

Dieses SLA ist Bestandteil des Hauptvertrages und gilt mit Vertragsschluss als akzeptiert. Eine gesonderte Unterzeichnung ist nicht erforderlich, sofern im Hauptvertrag nicht anders vereinbart.