SLA

SERVICE LEVEL AGREEMENT

Service Level Agreement

für die Nutzung der faktoora SaaS-Plattform

DSGVO · GoBD · ISO 27001 & SOC 2 Type II in Vorbereitung

VERSION	GÜLTIGKEIT	LETZTES REVIEW	NÄCHSTES REVIEW	VERANTWORTLICH
4.1	01.08.2026	09.07.2026	02.07.2027	faktoora GmbH – Geschäftsführung

Inhaltsverzeichnis

Verfügbarkeit der Plattform

4.1 Verfügbarkeitsgarantie

faktoora garantiert für alle Service-Tiers eine monatliche Mindest-Verfügbarkeit von 99,5 %.

Service-Tier	Verfügbarkeit/Monat	Max. Downtime/Monat	Max. Downtime/Jahr
Alle Service-Tiers	**99,5 %**	ca. 3,6 Stunden	ca. 43,8 Stunden

MESSMETHODIK

Verfügbarkeit wird über automatisierte Health-Checks aller Kernservices gemessen (internes Monitoring-System). Messzeitraum ist der Kalendermonat. Geplante Wartungsfenster werden ausgenommen. Kunden können jederzeit eine Statusabfrage per E-Mail anfordern; ein monatlicher Verfügbarkeitsbericht ist auf Anfrage erhältlich. Das Monitoring-System ist 24/7 aktiv und löst bei kritischen Incidents automatisch Alerts aus.

4.2 SLA-Credits bei Nichteinhaltung

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

Tatsächliche Verfügbarkeit	SLA-Credit
99,0 % bis < 99,5 %	**10 % der Monatsgebühr**
95,0 % bis < 99,0 %	**25 % der Monatsgebühr**
< 95,0 %	**50 % der Monatsgebühr**

Credits müssen innerhalb von 30 Tagen nach dem betreffenden Monat schriftlich bei support@faktoora.com beantragt werden. Sie sind auf die Monatsgebühr des betreffenden Zeitraums begrenzt.

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 CET
Telefon (Prio A/B)	+49 731 85070390	Mo–Fr, 09:00–17:00 Uhr CET
Sicherheitsvorfälle	security@faktoora.com	24/7 Eingang; priorisierte Bearbeitung gemäß Abschnitt 10

Geschäftszeiten: Montag bis Freitag, 09:00–17:00 Uhr CET, ausgenommen gesetzliche Feiertage in Bayern.

5.2 Prioritäten und Reaktionszeiten

Prio	Beschreibung	Reaktionszeit	Lösungszeit	Eskalation nach
A – Kritisch	Plattform vollständig ausgefallen oder Datenverlust. Kein Workaround.	1 Stunde	8 Stunden	2 Stunden
B – Hoch	Wesentliche Funktion beeinträchtigt, Workaround möglich.	4 Stunden	2 Geschäftstage	8 Stunden
C – Mittel	Funktionseinschränkung ohne kritische Auswirkung.	1 Geschäftstag	10 Geschäftstage	36 Stunden
D – Gering	Kosmetische Fehler, Verbesserungswünsche, allgemeine Anfragen.	2 Geschäftstage	Nach Planung / Best Effort	–

Alle Fristen gelten innerhalb der Geschäftszeiten (Mo–Fr 09:00–17:00 Uhr CET). Außerhalb der Geschäftszeiten beginnen die Fristen mit dem nächsten Geschäftstag. Prio A: Kritische Incidents werden durch automatisiertes Monitoring 24/7 erkannt und soweit möglich automatisch behandelt; die menschliche Reaktion erfolgt innerhalb von 1 Stunde ab Beginn der nächsten Geschäftszeiten.

5.3 Eskalationsverfahren

- Stufe 1 – Support-Team: Automatische Benachrichtigung bei Fristüberschreitung
- Stufe 2 – CTO: Einbeziehung bei anhaltender Nicht-Lösung, persönliche Rückmeldung an den Kunden
- Stufe 3 – Geschäftsführung: Bei kritischen oder wiederholten SLA-Verletzungen

Manuelle Eskalation jederzeit per E-Mail mit Betreff "ESKALATION: [Ticket-ID]" möglich.

Einleitung und Zweck

Dieses Service Level Agreement (SLA) der faktoora GmbH legt verbindliche Verpflichtungen zur Verfügbarkeit, Sicherheit, Betriebskontinuität und zum Supportbetrieb der faktoora SaaS-Plattform fest. Es ergänzt den Hauptvertrag sowie den Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO.

Das Dokument orientiert sich an den Anforderungen folgender Standards:

- ISO/IEC 27001:2022 – Informationssicherheits-Managementsystem (ISMS implementiert; Zertifizierung geplant)
- SOC 2 Type II – Trust Service Criteria (in Vorbereitung; Readiness-Mapping abgeschlossen)
- DSGVO – Datenschutz-Grundverordnung
- GoBD – Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern

> Das SLA gilt ausschließlich für zahlende Kunden mit aktivem Vertrag. Es findet keine Anwendung auf kostenfreie Testzugänge, sofern nicht ausdrücklich schriftlich vereinbart.

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, in dem die Plattform ordnungsgemäß funktioniert.
Downtime	Zeitraum vollständiger Nicht-Verfügbarkeit – exkl. geplanter Wartung und höherer Gewalt.
Geplante Wartung	Vorangekündigte Zeitfenster, in denen die Plattform eingeschränkt oder nicht verfügbar ist.
Reaktionszeit	Zeit zwischen Eingang einer Meldung und erster qualifizierter Rückmeldung durch faktoora.
Lösungszeit	Zeit zwischen Eingang einer Meldung und vollständiger Behebung.
RTO (Recovery Time Objective)	Maximale Zeitspanne vom Ausfall bis zur Wiederherstellung der Betriebsbereitschaft.
RPO (Recovery Point Objective)	Maximaler Datenverlust-Zeitraum; der älteste Wiederherstellungspunkt im Notfall.
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).

4.3 Ausschlüsse

Folgende Zeiträume zählen nicht als Downtime:

- Geplante Wartungsfenster gemäß Abschnitt 9
- Höhere Gewalt (Naturkatastrophen, Streik, staatliche Eingriffe)
- Ausfälle, die durch den Kunden oder Dritte verursacht wurden
- Netzwerkausfälle bei Internet Service Providern
- DDoS-Angriffe, die vereinbarte Schutzmechanismen überschreiten

Datensicherheit und Verschlüsselung

Die nachfolgenden Maßnahmen entsprechen den technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 DSGVO und sind an Anhang A der ISO/IEC 27001:2022 ausgerichtet.

6.1 Verschlüsselung

Bereich	Standard	Details
Daten at rest	**LUKS (AES)**	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.
Datenbank-Backups	**Verschlüsselte Backups (BorgBackup)**	Backups werden verschlüsselt gespeichert und über SSH übertragen.
Passwörter	**bcrypt (salted)**	Keine Klartextspeicherung. API-Schlüssel werden ebenfalls gehasht abgelegt.

6.2 Backup und Wiederherstellung

Parameter	Wert
Backup-Frequenz	Datenbank: stündlich; Dateispeicher: alle 2 Stunden; zusätzlich tägliches vollständiges System-Snapshot
Aufbewahrungszeit	14 Tage (Tages-Backups); bis zu 24 Monate (Monats-Backups)
RPO (Recovery Point Obj.)	Maximal 2 Stunden (Datenbank: 1 Stunde)
RTO (Recovery Time Obj.)	Maximal 8 Stunden für vollständige Plattform-Wiederherstellung; einzelne Dienste typischerweise deutlich schneller
Backup-Standort	ISO 27001-zertifizierte Rechenzentren in Deutschland (Hetzner)
Backup-Tests	Jährliche dokumentierte Restore-Tests; monatliche automatisierte Integritätsprüfung
Integritätsprüfung	Automatische Prüfsummen-Verifikation bei jedem Backup-Lauf

6.3 Redundanz und Hochverfügbarkeit

- Multi-Node-Cluster mit automatischem Neustart und Verlagerung ausgefallener Services
- 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

Zertifizierung / Standard	Scope	Status	Nachweis
ISO/IEC 27001:2022	ISMS der faktoora SaaS-Plattform	**In Vorbereitung**	Nach Abschluss auf Anfrage
SOC 2 Type II	Security, Availability, Confidentiality	**In Vorbereitung**	Nach Abschluss auf Anfrage (NDA)
ISO 27001 – RZ	Hosting-Infrastruktur	**Zertifiziert**	RZ-Zertifikat auf Anfrage
DSGVO / Art. 28	Auftragsverarbeitung	**Erfüllt**	AVV als Vertragsbestandteil
GoBD	Elektronische Buchführung	**Erfüllt**	Technische Dokumentation

faktoora stellt auf Anfrage verfügbare Zertifikate und Nachweise bereit. Sobald die ISO 27001- und SOC 2 Type II-Zertifizierungen abgeschlossen sind, werden die jeweiligen Prüfberichte auf Anfrage und nach Unterzeichnung einer NDA zur Verfügung gestellt.

7.2 SOC 2 Trust Service Criteria – Mapping

TSC-Kriterium	Abgedeckt durch
CC6 – Logical & Physical Access	Abschnitt 8: Zugriffskontrolle, MFA, Audit-Logs
CC7 – System Operations	Abschnitt 10: Incident Management; Abschnitt 9: Change Management
CC8 – Change Management	Abschnitt 9: Formaler Change-Prozess
A1 – Availability	Abschnitt 4: Verfügbarkeitsgarantie, SLA-Credits; Abschnitt 6: RTO/RPO
C1 – Confidentiality	Abschnitt 6: Verschlüsselung; Abschnitt 8: Zugriffsschutz
PI1 – Processing Integrity	Abschnitt 7.3: GoBD, Audit-Logs, manipulationserkennbare Speicherung (Hash-Kette)
P – Privacy	Abschnitt 11: DSGVO / AVV, Datenlokalisierung

7.3 GoBD-Konformität

- Manipulationserkennbarer Audit-Trail (append-only, kryptografische Hash-Kette)
- Vollständige Protokollierung aller Datenänderungen mit Zeitstempel und Benutzeridentifikation
- Datenexport in maschinenlesbaren Formaten (u. a. CSV, XLSX, XML) auf Anfrage
- Aufbewahrung gemäß gesetzlicher Fristen (10 Jahre für steuerrelevante Daten)

Zugriffskontrolle und Audit-Logging

8.1 Zugriffskontrolle (ISO 27001 A.5.15, SOC 2 CC6)

- Rollenbasiertes Zugriffsmodell (RBAC) nach Least-Privilege-Prinzip
- Mehrfaktorauthentifizierung für administrative Infrastrukturzugänge (SSH mit Schlüssel + Einmalpasswort, Cloud-Konsole, interne Entwicklersysteme)
- Vierteljährliche Überprüfung aller Produktions- und Entwicklerzugriffsrechte
- Sofortige 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 (ISO 27001 A.8.15, SOC 2 CC7)

- Protokollierung aller Authentifizierungsereignisse (Login, Logout, fehlgeschlagene Versuche)
- Protokollierung aller administrativen Systemänderungen
- Append-only Audit-Trail mit kryptografischer Hash-Kette; Manipulationen sind technisch erkennbar
- Aufbewahrung anwendungsbezogener Audit-Logs gemäß gesetzlicher Aufbewahrungsfristen (bis zu 10 Jahre)
- Auskunft über protokollierte eigene Daten im Rahmen der DSGVO-Betroffenenrechte

Change Management und Wartung

Alle Änderungen unterliegen einem formalen Change-Management-Prozess mit Review-Pflicht, Klassifizierung und Rollback-Fähigkeit, ausgerichtet an ISO 27001 A.8.32.

9.1 Wartungsfenster

Zeitfenster	Frequenz	Ankündigung
Geplante Wartung mit erwarteter Beeinträchtigung	Nach Bedarf; bevorzugtes Fenster Mo–Fr 18:00–22:00 Uhr oder Samstag	Mindestens 48 Stunden vorab per E-Mail

9.2 Notfall-Changes

- Kritische Sicherheits-Patches können ohne Vorankündigung eingespielt werden
- Information betroffener Kunden zeitnah, spätestens am folgenden Geschäftstag
- Incident-Report auf Anfrage verfügbar

9.3 Change-Typen

Change-Typ	Definition	Freigabe durch	Rollback-Plan
Standard Change	Routineänderung mit geringem Risiko	Review durch zweite Person (Merge Request)	Ja, dokumentiertes Verfahren
Significant Change	Änderung mit potenzieller Auswirkung auf Betrieb oder Sicherheit	Review + CTO-Freigabe	Ja, Rollback-Plan vor Deployment
Emergency Change	Kritischer Patch zur Schadensbegrenzung	Beschleunigtes Review; Information an CTO	Ja, dokumentiertes Verfahren

Sicherheitsvorfälle – Incident Management

Das Incident-Management entspricht ISO 27001 A.5.24–A.5.28 und SOC 2 CC7.3–CC7.5.

10.1 Klassifikation und Meldepflichten

Schweregrad	Beschreibung	Interne Reaktion	Kundenmeldung	Behördenmeldung
P1 – Kritisch	Datenverlust oder -abfluss personenbezogener Daten	System: sofort (24/7); Bewertung durch Person innerhalb 30 Min.	unverzüglich nach Feststellung, spätestens innerhalb von 4 Stunden ab Kenntniserlangung – auch außerhalb der Geschäftszeiten	72 Std. (Art. 33 DSGVO)
P2 – Hoch	Systemkompromittierung ohne bestätigten Datenverlust	Unverzüglich (Geschäftszeiten)	4 Stunden	Nach Risikoanalyse
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

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 innerhalb von 5 Geschäftstagen; zusammenfassender Bericht an betroffene Kunden auf Anfrage
- Lessons Learned: Erkenntnisse fließen in ISMS und Prozessdokumentation ein

10.3 Schwachstellenmanagement

- Kontinuierliche automatisierte Schwachstellen-Scans bei jeder Code-Änderung (Dependency-CVE-Scanning und statische Code-Analyse)
- Jährliche externe Penetrationstests durch qualifizierte Drittanbieter
- Risikobasierte, priorisierte Behebung: kritische Schwachstellen werden unverzüglich behandelt
- Penetrationstestergebnisse auf Anfrage einsehbar (unter NDA)

Datenschutz und Datenlokalisierung

- Hosting und Speicherung der Plattformdaten erfolgen in Rechenzentren in Deutschland
- Einzelne Unterauftragsverarbeiter (z. B. Zahlungsabwicklung) können Daten in Drittländern verarbeiten; Absicherung über EU-Standardvertragsklauseln (Art. 46 DSGVO); aktuelle Liste im AVV
- Auftragsverarbeitung geregelt im AVV gemäß Art. 28 DSGVO
- Beantwortung von Betroffenenanfragen (Art. 15–22 DSGVO) unverzüglich, spätestens innerhalb eines Monats (Art. 12 Abs. 3 DSGVO)
- Externer Datenschutzbeauftragter: PROLIANCE GmbH, datenschutzbeauftragter@datenschutzexperte.de

Audit-Rechte und Nachweispflichten

- Kunden haben das Recht auf eine jährliche Sicherheitsprüfung (eigene oder bevollmächtigte Dritte)

- Ankündigung mind. 30 Tage vorab; Durchführung innerhalb der Geschäftszeiten
- faktoora stellt auf Anfrage (unter NDA) verfügbare Nachweise bereit, insbesondere:
  - ISO 27001-Zertifikat des Rechenzentrums
  - TOM-Dokumentation gemäß Art. 32 DSGVO sowie Zusammenfassung des Statement of Applicability (ISO 27001)
  - ISO 27001- und SOC 2-Prüfberichte, sobald die Zertifizierungen abgeschlossen sind
  - Verfügbarkeitsstatistiken des vergangenen Jahres
  - Business Continuity und Disaster Recovery Plan (Zusammenfassung)
- Kosten für Audits über den jährlichen Umfang hinaus trägt der Kunde

Business Continuity und Disaster Recovery

faktoora betreibt ein Business-Continuity- und Disaster-Recovery-Management, ausgerichtet an ISO 27001 A.5.29–A.5.30 sowie DORA Art. 11–12.

Parameter	Zielwert
RTO – Gesamtplattform	Maximal 8 Stunden
RTO – Einzelne Dienste	Typischerweise unter 1 Stunde (automatische Wiederherstellung)
RPO	Maximal 2 Stunden (Datenbank: 1 Stunde)
DR-Tests	Mind. 1× jährlich, dokumentiert
BCP-Review	Jährlich oder nach wesentlichen Systemänderungen
Backup-Ebenen	Zwei unabhängige Backup-Ebenen (verschlüsselte Daten-Backups und tägliche System-Snapshots)

Reporting und Transparenz

- Monatlicher Verfügbarkeitsbericht auf Anfrage (inkl. Wartungszeiten, tatsächliche Uptime)
- Jährliche Zusammenfassung der Sicherheitskennzahlen auf Anfrage (Incidents, Schwachstellenbehandlung, Backup-Tests)
- Benachrichtigung betroffener Kunden bei Incidents per E-Mail gemäß Abschnitt 10

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.

Gültigkeit, Änderungen und Sonderkündigungsrecht

- Dieses SLA gilt für die Dauer des zugrundeliegenden Hauptvertragsverhältnisses
- faktoora überprüft das SLA mindestens einmal jährlich
- Änderungen werden mindestens 30 Tage vor Inkrafttreten per E-Mail mitgeteilt
- Bei Nichtakzeptanz steht dem Kunden ein außerordentliches Kündigungsrecht innerhalb von 30 Tagen zu
- Das jeweils aktuelle SLA ist unter faktoora.com/legal abrufbar