HIDORA SA – ALLGEMEINE GESCHÄFTSBEDINGUNGEN

Interne Referenz: 001-GC Hidora FR1 — Ausgabe: Oktober 2025
HIDORA SA (CHE-286.910.173) – Avenue des Morgines 12, 1213 Petit-Lancy, Schweiz
Website: https://hidora.io/

Diese Allgemeinen Geschäftsbedingungen («AGB») regeln sämtliche Leistungen von HIDORA SA («HIDORA»), die dem Kunden (juristische oder natürliche Person, die im Rahmen ihrer beruflichen Tätigkeit handelt) erbracht werden, insbesondere Cloud-Infrastruktur- und Plattformdienste (IaaS/PaaS), Managed Services, Beratung, Projektleistungen, Wartung und zugehörige Dienste (zusammen die «Dienste»). Diese AGB, die Besonderen Bedingungen sowie die Bestellung(en), Offerten, Bestellscheine, SOW/Projekt(e) und deren Anhänge (zusammen der «Vertrag») bilden die vollständige Vereinbarung zwischen den Parteien.

Inhaltsverzeichnis

1. Wesentliche Definitionen

Kundenzugang	Zugangsdaten (Login, MFA, API-Schlüssel), die die Administration der Dienste ermöglichen.
Administrator	Vom Kunden benannter Benutzer mit Verwaltungsrechten für das Konto und die Kundenzugänge.
AUP	Richtlinie zur akzeptablen Nutzung von HIDORA (Anhang A).
Affiliate	Einheit, die eine Partei kontrolliert, von einer Partei kontrolliert wird oder unter gemeinsamer Kontrolle mit einer Partei steht (Kontrolle ≥ 50 % der Stimmrechte oder effektive Leitung).
Beta/Preview	Vorkommerzielle Testfunktionen ohne Garantien, die sich ändern oder zurückgezogen werden können.
Business Day/Arbeitstag	Montag–Freitag (ohne offizielle Feiertage am Sitz von HIDORA).
Kontrollwechsel	Vorgang, der die Kontrolle über mehr als 50 % des Kapitals oder der Stimmrechte einer Partei verändert.
Bestellung	Unterzeichneter Bestellschein/Offerte oder Online-Bestätigung, welche das Angebot, die Dauer, die Mengen, die Preise und die besonderen Bedingungen des betreffenden Dienstes beschreibt.
Konto	Kundenbereich zur Verwaltung der Dienste und der Kundenzugänge, der bei Abschluss des Vertrags erstellt wird.
Besondere Bedingungen	Servicespezifische Bedingungen, die in der Bestellung und/oder dem Service-Datenblatt aufgeführt sind und die vorliegenden AGB ergänzen und im Widerspruchsfall gegenüber diesen vorrangig gelten.
Inhalt	Daten, Codes, Dateien, Konfigurationen, Protokolle und Metadaten, die vom Kunden über die Dienste bereitgestellt oder erzeugt werden.
Dienstgutschriften	Im SLA vorgesehene Gutschriften bei Nichtverfügbarkeit.
Deliverables / Lieferobjekte	Spezifische Ergebnisse einer Projekt-/IT-Betrieb-/Beratungsleistung, die in einer SOW beschrieben sind.
Personendaten	Alle Daten im Sinne des schweizerischen Rechts (DSG) und/oder der DSGVO, die von HIDORA als Auftragsbearbeiter verarbeitet werden.
Besonders schützenswerte Personendaten	Bezeichnet die besonderen Kategorien von Daten im Sinne des schweizerischen Rechts (insbesondere Art. 5 lit. c DSG) und gegebenenfalls der DSGVO, insbesondere Daten über die Gesundheit, biometrische und genetische Daten, die eine Person identifizieren können, religiöse, philosophische, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Massnahmen der sozialen Hilfe, strafrechtliche oder administrative Verfolgungen und Sanktionen sowie alle anderen Daten, die das Gesetz als besonders schützenswert qualifiziert.
Umgebung	Infrastruktur, Rechenzentren, Software, Netzwerke und technische Elemente, die von HIDORA und seinen Subunternehmern betrieben werden.
Incident / Störung	Ereignis, das die Verfügbarkeit, die Leistung, die Sicherheit oder die Integrität der Dienste beeinträchtigt.

Wartungsfenster	Geplantes Zeitfenster, in dem HIDORA Wartungsarbeiten durchführen kann, die die Verfügbarkeit der Dienste vorübergehend beeinträchtigen können. Die geltenden Wartungsfenster werden auf dem Portal/Service-Datenblatt veröffentlicht und können mit angemessener Vorankündigung angepasst werden.
Notice & Action	Verfahren zur Behandlung von Meldungen über rechtswidrige Inhalte oder Rechtsverletzungen, wie in **Anhang C** beschrieben.
Projekt	Strukturierte Leistung, beschrieben in einer SOW/einem Projektplan (Meilensteine, Lieferobjekte, Abnahmekriterien).
Site / Portal	Internetseiten und Kundenportale von HIDORA (einschliesslich Ticketsystem), die für die Buchung und den Support der Dienste genutzt werden.
SLA	Service-Verpflichtungen/SLA-Veröffentlichungen von HIDORA (Link angegeben in Anhang B).
Weiterer Unterauftragsbearbeiter	Von HIDORA beauftragter Dienstleister zur Bearbeitung von Personendaten im Auftrag des Kunden.
Benutzer	Jede vom Kunden autorisierte Person zur Nutzung der Dienste.

2. Technische Definitionen

SOW (Statement of Work)	Dokument, das den Umfang, die Liefergegenstände, die Meilensteine, die Abnahmekriterien und die spezifischen Bedingungen eines Projekts oder einer Managed-Service-Leistung beschreibt.
IaaS (Infrastructure as a Service)	Bereitstellung virtualisierter IT-Infrastrukturen (Server, Speicher, Netzwerk), die von HIDORA verwaltet werden und die der Kunde aus der Ferne administriert.
PaaS (Platform as a Service)	Gemäßigte Anwendungsplattform, die die Bereitstellung und Verwaltung von Anwendungen ermöglicht, ohne dass die zugrunde liegenden Ressourcen direkt verwaltet werden müssen.
DRaaS (Disaster Recovery as a Service)	Dienst zur Wiederaufnahme des Betriebs und zur Wiederherstellung kritischer Systeme nach einem Schadenfall, gemäss den in der Bestellung oder der SOW festgelegten Parametern.
SaaS (Software as a Service)	Softwareanwendung, die von HIDORA gehostet wird und auf die der Kunde gemäss den vertraglichen Bedingungen aus der Ferne zugreifen kann.
PAYG (Pay-As-You-Go)	Abrechnungsmodell nach tatsächlichem Verbrauch, ohne feste Verpflichtung.
API (Application Programming Interface)	Software-Schnittstelle, die es dem Kunden ermöglicht, programmatisch mit den Diensten zu interagieren.
Backup as a Service (BaaS)	Verwalteter Backup-Dienst, der Kopien der Kundendaten hostet, getrennt vom DRaaS.

3. Regeln zur Auslegung der Definitionen

3.1 Die Begriffe «**einschliesslich**» oder «**insbesondere**» gelten ohne Einschränkung.

3.2 Titel haben keinen Einfluss auf die Auslegung.

3.3 Verweise auf einen Rechtstext beziehen sich auf jede geänderte oder ersetzte Fassung.

3.4 Elektronische Mitteilungen gelten als Schriftform.

4. Vertragshierarchie und Referenzsprache

4.1 **Hierarchie.** Im Falle eines Widerspruchs gilt folgende Rangordnung: (i) Besondere Bedingungen eines Dienstes oder SOW/Projekt, (ii) Bestellung(en), (iii) vorliegende AGB, (iv) kommerzielle Dokumente. Dokumente niedrigeren Ranges sind ergänzend zu jenen höheren Ranges auszulegen.

4.2 **Versionen und Sprache.** Sofern nichts anderes vereinbart, ist die französische Fassung massgebend. Übersetzungen werden als Gefälligkeit zur Verfügung gestellt.

4.3 **Dokumentenevolution.** Anhänge operationeller Natur (SLA, AUP, Verzeichnis der weiteren Unterbeauftragten, Verfahren) können aus rechtlichen, technischen oder sicherheitsbezogenen Gründen aktuell gehalten werden; jede wesentliche Änderung, die geeignet ist, die wesentlichen Rechte des Kunden nachteilig zu beeinflussen, wird mit angemessener Vorankündigung mitgeteilt und gilt nur für die Zukunft.

5. Vertragsabschluss – Konto und Organisation

5.1 **Vertragsbeginn.** Der Vertrag tritt beim ersten der folgenden Ereignisse in Kraft: (i) Erstellung eines Kontos und Annahme der AGB, (ii) Unterzeichnung einer Bestellung/SOW, (iii) Zugang zu oder Nutzung der Dienste.

1.1 Der Kunde erstellt ein **Konto** und benennt mindestens einen **Administrator.** Der Kunde bleibt verantwortlich für alle Handlungen, die über die Kundenzugänge vorgenommen werden, einschliesslich durch seine Benutzer, Dienstleister und Personen unter seiner Kontrolle. Der Kunde richtet eine starke Authentifizierung (MFA) sowie minimale Berechtigungen ein.

5.2 HIDORA kann jederzeit Identitäts- und Adressprüfungen durchführen, wenn dies aus Gründen der Sicherheit, zur Betrugs- oder Geldwäschereibekämpfung, im Rahmen von Sanktionsregelungen, Exportkontrollen oder Compliance erforderlich ist.

5.3 Die **Affiliates** des Kunden können die Dienste über denselben Vertrag nutzen (sofern in der Bestellung angegeben); der Kunde bleibt solidarisch haftbar für deren Handlungen.

6. Beschreibung der Dienste

6.1 **Cloud IaaS/PaaS.** Die Cloud-Umgebung von HIDORA wird hauptsächlich in der Schweiz betrieben, mit Redundanz und geplanten Wartungsarbeiten. Die Eigenschaften der Angebote sind auf dem Portal/Kundenbereich und/oder in der Bestellung aufgeführt. HIDORA kann die Umgebung weiterentwickeln (Hardware-/Software-Upgrade, Patching), ohne die Funktionalität oder Sicherheit wesentlich zu beeinträchtigen.

6.2 **Projekte, Managed Services und Beratung.** Projekt-, Managed-Service- und Beratungsleistungen werden gemäss einer SOW/Projektplan (Meilensteine, Liefergegenstände, Abnahmekriterien) erbracht. Die angegebenen Fristen sind indikativ.

6.3 **Support.** HIDORA stellt Support über das Portal/Ticketsystem sowie über eine Hotline während der veröffentlichten Zeiten bereit, mit allfälligen zusätzlichen Supportstufen entsprechend Angebot.

6.4 **Drittsoftware und Open-Source.** Einige Dienste basieren auf Drittsoftware oder Open-Source-Komponenten. Der Kunde akzeptiert deren Lizenzbedingungen; im Konfliktfall haben diese Lizenzen für die betreffende Komponente Vorrang. HIDORA übernimmt keine Drittgarantien über die vom Anbieter gewährten Bedingungen hinaus.

6.5 **Beta/Preview.** Funktionen in Beta-/Preview-Version werden «wie sie sind» bereitgestellt, ohne Verfügbarkeits-, Leistungs- oder Reversibilitätsgarantie.

6.6 **Geplante und Notfallwartung.** HIDORA kann Eingriffe während der veröffentlichten Maintenance Windows durchführen. Im Falle einer Notfallwartung (Sicherheit, Stabilität) handelt HIDORA mit bestmöglicher angemessener Vorankündigung und begrenzt die Auswirkungen. Wartungszeiträume, die den veröffentlichten Maintenance Windows entsprechen (oder im Notfall ordnungsgemäss mitgeteilt wurden), werden bei der Berechnung der Verfügbarkeit gemäss SLA ausgeschlossen.

7. Nutzung der Dienste – AUP und Sicherheit

7.1 Der Kunde hält jederzeit die **AUP** (Anhang A) ein: Verbot rechtswidriger oder gegen die öffentliche Ordnung verstossender Aktivitäten (darunter, ohne Einschränkung: Malware, SPAM, Verletzung von Rechten Dritter und von Persönlichkeitsrechten, Betrug, Angriffe auf Systeme, Umgehung von Filtern, unzulässiges Hosting zum Weiterverkauf usw.).

7.2 HIDORA kann einen Dienst suspendieren oder einschränken bei Vertragsverletzung, Sicherheitsvorfall, Bedrohung für die Umgebung oder auf Anfrage von Behörden oder glaubwürdigen Dritten; HIDORA informiert den Kunden in zumutbarem Umfang und gibt die erforderlichen Korrekturmassnahmen an.

7.3 Der Kunde gewährleistet eine sichere **Konfiguration** (Firewall, IAM, Rotation von Secrets, clientseitige Verschlüsselung, Backups, OS-Härtung) und stellt die Rechtmässigkeit seines Inhalts sicher. HIDORA stellt dem Stand der Technik entsprechende organisatorische und technische Massnahmen zum Schutz der Umgebung bereit.

7.4 **Persönlichkeit und rechtswidrige Inhalte.** Der Kunde garantiert, dass sein Inhalt keine Persönlichkeitsrechte verletzt (Bild, Stimme, besonders schützenswerte Personendaten), keine Urheber- oder Markenrechte, keine Geschäftsgeheimnisse und keine strafrechtlichen Bestimmungen. HIDORA wendet einen **Notice-&-Action-Mechanismus (Anhang C)** für Ansprüche Dritter an; bei offensichtlichem Risiko kann HIDORA die strittigen Elemente vorläufig entfernen oder suspendieren.

8. Datenschutz und Vertraulichkeit

8.1 **Rollen.** Der Kunde handelt als Verantwortlicher für die Bearbeitung seiner Personendaten; HIDORA handelt als Auftragsbearbeiter im Sinne des DSG und gegebenenfalls der DSGVO.

8.2 **DPA.** Die Bestimmungen von **Anhang D** (DPA/Auftragsbearbeitung) sind integraler Bestandteil des Vertrags (Gegenstand, Dauer, Datenkategorien, Kategorien betroffener Personen, Weisungen, Sicherheit, Vertraulichkeit, Unterstützung, Verzeichnis der Unterbeauftragten, Übermittlungen, angemessene Audits/Assessments, Meldung von Sicherheitsvorfällen, Löschung/Rückgabe).

8.3 **Lokalisierung.** Sofern nichts anderes vereinbart ist, erfolgt das Haupthosting in der Schweiz. Damit verbundene Bearbeitungen (z. B. Anti-DDoS, Monitoring, Support, Datensicherungen) können aufgelistete und vertraglich gebundene Unterbeauftragte einbeziehen. Übermittlungen ausserhalb der Schweiz bzw. des EWR stützen sich – sofern anwendbar – auf einen anerkannten Mechanismus (EU-Standardvertragsklauseln mit schweizerischem Addendum oder Angemessenheitsentscheid), mit ergänzenden Massnahmen.

8.4 **Vertraulichkeit.** Jede Partei schützt die vertraulichen Informationen der anderen während der Vertragsdauer und **3 Jahre** nach dessen Beendigung (unbeschadet der Geschäftsgeheimnisse, die geschützt bleiben, solange sie geheim sind). Die Verpflichtungen gelten nicht für öffentliche Informationen, rechtmässig von einem Dritten erhaltene oder unabhängig entwickelte Informationen. Die nicht auf Personendaten bezogene Vertraulichkeit wird durch Anhang E (Vertraulichkeit) geregelt, der im Falle einer Abweichung von diesem Artikel Vorrang hat.

9. Datensicherung, Kontinuität und Reversibilität

9.1 **Datensicherungen.** Sofern keine andere Option bzw. kein entsprechendes Abonnement vereinbart ist, obliegen die applikativen Datensicherungen dem Kunden. HIDORA kann Backup- oder DRaaS-Angebote gemäss Besonderen Bedingungen anbieten.

9.2 **Reversibilität.** Bei Vertragsende kann der Kunde die Rückgabe seines Inhalts in einem angemessenen Standardformat verlangen; Gebühren können anfallen. Sofern nichts anderes vereinbart ist, bewahrt HIDORA den Inhalt während dreissig (30) Tagen ab Ablauf oder Kündigung auf, um dessen Wiederherstellung durch den Kunden zu ermöglichen, und löscht ihn anschliessend endgültig innerhalb der darauffolgenden dreissig (30) Tage. Die technischen Modalitäten der Rückgabe und Löschung sind in Art. 11 Anhang D – «Rückgabe und Löschung der Daten» – präzisiert.

10. Gebühren, Rechnungsstellung und Steuern

10.1 Die Tarife (ohne Steuern) sind in der Bestellung bzw. im Portal aufgeführt, je nach gewähltem Modell (Abonnement, PAYG, Gutschriften, Stunden-/Personentage). Steuern, Import-/Exportabgaben, Gebühren und Bankspesen gehen zu Lasten des Kunden.

10.2 Sofern in der Bestellung oder den Besonderen Bedingungen nichts anderes vereinbart ist:

a) **Wiederkehrende Leistungen** – Wiederkehrende Dienste (Hosting, Wartung, Support usw.) werden im Voraus, auf monatlicher, quartalsweiser oder jährlicher Basis entsprechend der vereinbarten Periodizität in Rechnung gestellt.

b) **Projekt- oder Beratungsleistungen** – Einmalige Leistungen wie Projektarbeit, Deployment, Integration oder Beratung können nach einem der folgenden Modelle abgerechnet werden :

- **Pauschale nach Meilensteinen:** 50 % bei Bestellung oder Projektstart und 50 % bei Lieferung oder Inbetriebnahme, sofern in der Bestellung nichts anderes angegeben ist ;
- **Nach Aufwand:** Basierend auf der tatsächlich geleisteten Zeit, gemäss den geltenden Stundensätzen oder Tagessätzen, periodisch in Rechnung gestellt (in der Regel Ende Monat) ;
- **Vorausbezahltes Pauschalvolumen («Tageskontingent»):** Vorauszahlung der vereinbarten Anzahl Tage oder Einheiten, die dann fortlaufend verbraucht werden.

c) **Zahlungsbedingungen.** Rechnungen sind netto innerhalb von **30 Tagen** nach Rechnungsstellung zahlbar, sofern keine andere Fälligkeit ausdrücklich vereinbart wurde. HIDORA behält sich das Recht vor, die Erbringung der Dienste bei Nichtzahlung zum Fälligkeitstermin auszusetzen.

10.3 **Verzug.** Bei Zahlungsverzug von mehr als 30 Tagen kann HIDORA: (i) die Dienste nach schriftlicher Vorankündigung von mindestens zehn (10) Kalendertagen aussetzen, ausser bei Dringlichkeit oder Gefahr für die Umgebung, wobei HIDORA das Recht vorbehalten bleibt, Zahlungssicherheiten zu verlangen; (ii) die vorzeitige Fälligkeit der geschuldeten Beträge verlangen; (iii) übliche Verzugszinsen und Betreibungskosten erheben. Bereits gezahlte Beträge werden nicht zurückerstattet.

10.4 HIDORA kann die Tarife für Verlängerungszeiträume anpassen; die Änderungsmitteilung erfolgt über das Portal und/oder per E-Mail.

10.5 **Drittprodukte.** Die Preise und Bedingungen von Drittanbietern/Herstellern gelten und haben für den betreffenden Teil Vorrang.

11. Garantien

11.1 **Cloud.** Die Cloud-Dienste werden **„wie sie sind“** bereitgestellt, vorbehaltlich der im anwendbaren SLA vereinbarten Serviceverpflichtungen.

11.2 **Projekte/Beratung.** HIDORA erbringt diese Leistungen mit der Sorgfalt und dem Fachwissen eines erfahrenen Professionals und liefert die **Liefergegenstände** entsprechend der SOW zum Zeitpunkt der Lieferung. **Garantiezeitraum:** 60 Tage ab formeller Abnahme; HIDORA korrigiert nachweisbare Mängel, die auf eigenes Verschulden zurückzuführen sind, angemessen.

11.3 HIDORA **garantiert weder einen** unterbrechungsfreien oder fehlerfreien Betrieb noch die vollständige Abwesenheit unbefugter Zugriffe oder Angriffe Dritter; Termine und Zeitangaben sind indikativ.

12. Laufzeit, Aussetzung und Kündigung

12.1 **Laufzeit.** Die Laufzeit ist in der Bestellung bzw. im Portal angegeben. Abgelaufene Abonnements führen zur automatischen **Aussetzung**, sofern keine Erneuerung erfolgt.

12.2 **Aussetzung.** HIDORA kann die Dienste ganz oder teilweise aussetzen bei schwerwiegendem Verstoss, Sicherheitsrisiko, Betrug, Nichtzahlung, Behördenanfrage oder Gefährdung der Umgebung; die Aussetzung berührt die geschuldeten Beträge nicht.

12.3 **Kündigung aus wichtigem Grund.** Ist der Verstoss behebbar, teilt HIDORA die zu ergreifenden Massnahmen innerhalb einer angemessenen Frist mit; andernfalls kann HIDORA den Vertrag von Rechts wegen kündigen. Der Kunde kann kündigen, wenn HIDORA eine wesentliche Verletzung innerhalb einer angemessenen Frist nicht behebt.

12.4 **Kontrollwechsel.** HIDORA informiert den Kunden mindestens dreissig (30) Tage vor Wirksamwerden eines ihn betreffenden Kontrollwechsels, soweit gesetzlich zulässig. Weist der Kunde eine wesentliche nachteilige Auswirkung auf die Sicherheit, Vertraulichkeit oder regulatorische Compliance seiner **Datenverarbeitungen** nach, und unterbreitet HIDORA innerhalb einer angemessenen Frist keine zumutbare kommerzielle Lösung, kann der Kunde den Vertrag **ohne Strafe** innerhalb von dreissig (30) Tagen nach Mitteilung kündigen; nicht genutzte vorausbezahlte Gebühren werden anteilsmässig zurückerstattet.

12.5 **Vertragsende und Daten.** Bei Ablauf oder Kündigung wird der Zugang ausgesetzt; sofern keine gesetzliche Aufbewahrungspflicht besteht, werden verbleibende Daten nach den angegebenen technischen Fristen endgültig gelöscht (siehe Anhang D). Der Kunde ist allein verantwortlich für die **vorherige Sicherung** seines Inhalts.

13. Geistiges Eigentum und Lizenzen

13.1 **Eigentümerschaft.** Der Kunde behält alle Rechte an seinem Inhalt. HIDORA behält alle Rechte an der Umgebung, ihrer Dokumentation, ihren Vorlagen, Skripten, Tools und ihrem Know-how, einschliesslich der während der Vertragsausführung entwickelten.

13.2 **Gegenseitige Lizenzen.** Jede Partei räumt der anderen für die Vertragsdauer und weltweit eine nicht ausschliessliche und nicht übertragbare Lizenz ein, die strikt auf die Vertragsausführung beschränkt ist.

13.3 **Drittanbieter-Software / Open Source.** In die Dienste integrierte Dritt- und Open-Source-Komponenten unterliegen weiterhin ihren eigenen Lizenzen, die für die betreffende Komponente Vorrang haben; HIDORA gewährt keine Garantie über die des Herausgebers hinaus.

13.4 **Beschränkungen.** Sofern keine zwingende gesetzliche Vorschrift entgegensteht, unterlässt der Kunde jegliches Reverse Engineering, jede Umgehung technischer Schutzmassnahmen und bewahrt die bestehenden Rechtshinweise.

13.5 **Feedback.** Vorschläge und Rückmeldungen des Kunden können von HIDORA frei zur Verbesserung der Dienste genutzt werden, ohne Lizenzgebühren oder Verpflichtungen und ohne Offenlegung vertraulicher Informationen des Kunden.

14. Haftung und Haftungsgrenzen

14.1 **Haftung.** Im Rahmen zwingender schweizerischer Gesetzesbestimmungen ist die gesamthaft kumulierte Haftung von HIDORA, aus sämtlichen Gründen zusammengenommen, auf den jeweils höheren Betrag begrenzt von: (i) dem tatsächlich vom Kunden für den verursachenden Dienst in den letzten sechs Monaten vor Eintritt des schädigenden Ereignisses gezahlten Betrag, oder (ii) CHF 50'000.–.

14.2 HIDORA haftet niemals für indirekte oder Folgeschäden (Gewinnverlust, Geschäftsausfall, Imageschaden, nicht durch den Kunden gesicherte Daten, entgangene Einsparungen, Ersatzkosten) oder für Schäden verursacht durch: (i) Elemente, die nicht von HIDORA bereitgestellt wurden, (ii) Nutzung entgegen den Anweisungen oder der AUP, (iii) Verschulden des Kunden oder seiner Dienstleister, (iv) Fälle von höherer Gewalt.

14.3 Nichts schliesst die Haftung von HIDORA bei nachgewiesenem Vorsatz oder grober Fahrlässigkeit aus.

14.4 Die im SLA vorgesehenen Dienstgutschriften stellen, sofern anwendbar, den alleinigen und ausschliesslichen Rechtsbehelf des Kunden bei Nichtverfügbarkeiten dar.

15. Compliance, Sanktionen und Ethik

15.1 **Allgemeine Compliance.** Jede Partei hält die anwendbaren Gesetze ein (Schweiz und gegebenenfalls EU), insbesondere in Bezug auf Datenschutz (DSG/DSGVO), Telekommunikation, Sanktionen/Exportkontrollen, Korruptionsbekämpfung, Geldwäscherei, Wettbewerb, geistiges Eigentum und Persönlichkeitsrechte.

15.2 **Sanktionen / Export.** HIDORA kann einen Dienst verweigern, aufschieben oder aussetzen, wenn dessen Erbringung gegen ein Sanktions- oder Exportkontrollregime oder gegen eine sonstige gesetzliche Verpflichtung verstossen würde. Der Kunde verpflichtet sich, die Dienste nicht an sanktionierte Nutzer oder Jurisdiktionen umzuleiten.

15.3 **Ethik.** Die Parteien untersagen jede Form von Korruption, Einflussnahme und vergleichbaren Praktiken, treffen Präventionsmassnahmen und richten einen geeigneten Meldemechanismus ein.

15.4 **Regulatorische Zusammenarbeit.** Soweit rechtlich und sicherheitsmässig zulässig, arbeitet jede Partei in angemessenem Umfang mit den zuständigen Behörden zusammen und informiert die andere Partei, wenn eine Compliance-Anforderung die Ausführung des Vertrags beeinflusst.

16. Nachweis, Protokollierung und eingeschränkte Audits

16.1 **Beweisvereinbarung.** Die Systemprotokolle, Metriken, Tickets, Zeitstempel und technischen Aufzeichnungen von HIDORA gelten zwischen den Parteien als Beweis, vorbehaltlich des Gegenbeweises durch den Kunden.

16.2 **Audits im Zusammenhang mit dem DPA.** Nach angemessener Vorankündigung und während der üblichen Geschäftszeiten ermöglicht HIDORA dokumentarische Überprüfungen im Zusammenhang mit Anhang D (DPA). Ein physischer Besuch der Rechenzentren ist nicht geschuldet, ausser bei zwingender regulatorischer Anforderung.

16.3 **Aufbewahrung.** HIDORA kann die für Beweis-, Sicherheits- und Compliance-Zwecke unbedingt erforderlichen Elemente für die notwendige Dauer aufbewahren.

17. Höhere Gewalt

17.1 **Grundsatz.** Keine Partei haftet für nicht-monetäre Pflichtverletzungen, die durch ein Ereignis verursacht werden, das vernünftigerweise ausserhalb ihrer Kontrolle liegt (z. B. schwerer Stromausfall, Rechenzentrums-Schaden, massive Cyberangriffe, Epidemie/Pandemie, behördliche Massnahme, Konflikt, Naturkatastrophe).

17.2 **Pflichten der betroffenen Partei.** Die betroffene Partei informiert die andere Partei innerhalb einer angemessenen Frist, ergreift Minderungsmassnahmen und nimmt die Vertragserfüllung wieder auf, sobald das Hindernis beseitigt ist.

17.3 **Zahlungen.** Fällige Geldverpflichtungen bleiben trotz höherer Gewalt bestehen.

18. Abtretung und Unteraufträge

18.1 **Abtretung.** Keine Partei darf den Vertrag ohne vorherige schriftliche Zustimmung der anderen Partei abtreten, ausser: (i) Forderungsabtretung durch HIDORA, (ii) Abtretung im Rahmen einer Reorganisation oder eines Geschäftsverkaufs (Universalübertragung); in diesen Fällen genügt eine Mitteilung.

18.2 **Unterbeauftragung.** HIDORA kann die Erbringung der Dienste ganz oder teilweise an Subunternehmer delegieren, bleibt jedoch für deren Handlungen verantwortlich, gemäss Anhang D (Verzeichnis der Unterauftragsbearbeiter und Datenschutzanforderungen).

19. Benachrichtigungen

19.1 **Mitteilungen.** Vertragliche Mitteilungen erfolgen wirksam schriftlich an die Postadresse des Sitzes und/oder an die im Konto angegebene E-Mail-Adresse. Operative Kommunikation kann über das Portal/Ticketsystem erfolgen.

19.2 **Empfang.** Sofern kein Gegenbeweis erbracht wird: (a) Eine E-Mail gilt am Arbeitstag des Versands als zugegangen; (b) Ein Einschreiben gilt spätestens am dritten Arbeitstag nach Versand als zugegangen.

19.3 **Geschäftliche Referenzen.** Sofern der Kunde nicht schriftlich widerspricht, darf HIDORA den Namen und das Logo des Kunden als Referenz verwenden (ohne Offenlegung vertraulicher Informationen). Der Kunde kann jederzeit per E-Mail an **legal@hidora.io** der Nutzung widersprechen; HIDORA hält sich an die vom Kunden kommunizierten Richtlinien zur Logo-Verwendung.

20. Verschiedenes

20.1 **Unabhängigkeit der Parteien.** Es besteht kein Unterordnungsverhältnis oder generelles Mandat.

20.2 **Nichtverzicht.** Dass eine Partei ein Recht nicht geltend macht, gilt nicht als Verzicht auf dieses Recht.

20.3 **Salvatorische Klausel.** Die Ungültigkeit einer Klausel berührt nicht die Gültigkeit der übrigen Bestimmungen; die ungültige Klausel wird durch eine gültige Klausel ersetzt, die der Absicht der Parteien möglichst nahekommt.

20.4 **Gesamte Vereinbarung.** Der Vertrag hebt alle vorherigen Vereinbarungen zu seinem Gegenstand auf und ersetzt sie.

21. Geltendes Recht und Gerichtsstand

21.1 **Anwendbares Recht und Gerichtsstand.** Der Vertrag unterliegt schweizerischem Recht, unter Ausschluss des Wiener Übereinkommens über den internationalen Warenkauf (CISG/UN-Kaufrecht).

21.2 **Ausschliesslicher Gerichtsstand.** Ausschliesslicher Gerichtsstand ist Genf, vorbehaltlich der Rechtsmittel vor dem Bundesgericht nach anwendbarem Recht.

Oktober 2025

Anhang A – Richtlinie zur akzeptablen Nutzung (AUP)

1. Gegenstand und Geltungsbereich

Die vorliegende Richtlinie zur akzeptablen Nutzung regelt jede Nutzung der Dienste durch den Kunden, seine Benutzer, seine Unterbeauftragten und seine Affiliates.

Sie ergänzt die Allgemeinen Geschäftsbedingungen und die Besonderen Bedingungen. Jeder Verstoss gegen die AUP stellt eine Vertragsverletzung dar.

2. Allgemeine Grundsätze

Der Kunde nutzt die Dienste rechtmässig, sicher und verantwortungsvoll. Er unterlässt Handlungen, die die von HIDORA betriebene Umgebung, andere Kunden oder Dritte beeinträchtigen könnten.

Der Kunde wahrt jederzeit die Persönlichkeitsrechte, das geistige Eigentum und die anwendbaren Datenschutzbestimmungen.

3. Rechtswidrige oder schädliche Inhalte

Der Kunde darf keine Inhalte hosten, übermitteln, veröffentlichen oder zugänglich machen, die gegen Urheberrechte verstossen, ein Geschäftsgeheimnis verletzen oder Persönlichkeitsrechte beeinträchtigen, einschliesslich des Rechts am eigenen Bild, der Stimme oder besonders schützenswerter Personendaten Dritter.

Ebenfalls untersagt sind diffamierende, hetzerische, diskriminierende, gewaltverherrlichende, terroristische, belästigende oder bedrohliche Inhalte sowie jegliche kinderpornografische Inhalte oder Inhalte, die zur Begehung von Straftaten aufrufen.

Der Kunde unterlässt jegliches Phishing, jeden Betrug, jeden Identitätsdiebstahl und jede sonstige täuschende Manipulation.

Er stellt allgemein sicher, dass sämtliche seiner Aktivitäten den anwendbaren Gesetzen entsprechen, insbesondere jenen betreffend Telekommunikation, Glücksspiel, regulierte Waren und Dienstleistungen sowie Werbung.

4. Verbotene technische Aktivitäten

Der Kunde unterlässt die Verbreitung von Schadsoftware (einschliesslich Ransomware, Backdoors und Botnets), die Durchführung von Angriffen oder Angriffsversuchen gegen Systeme (wie Massenscans, Brute Force, DDoS/DoS, Amplifikationsangriffe, Injections, XSS, SSRF, Privilegienerweiterungen, Abfangen oder Umleitung von Datenverkehr) sowie die Umgehung oder Neutralisierung von Sicherheitsmechanismen wie WAF, IDS/IPS, Zugangskontrolllisten oder Quotas.

Er betreibt keine Open Relays, Open Resolver oder ungesicherte anonyme Proxys.

Er verkauft die Dienste nicht ohne Genehmigung weiter und betreibt kein «Bulletproof»-Hosting.

Jede Nutzung, die darauf abzielt, die Verfügbarkeit oder Leistung der Umgebung, der Dienste oder Dritter zu stören, ist untersagt.

5. Sicherheit und Identity-Management

Im Rahmen eines Shared-Responsibility-Modells setzt HIDORA technische und organisatorische Massnahmen zum Schutz der Umgebung um.

Der Kunde implementiert eine Mehrfaktor-Authentifizierung für administrative Profile, wendet Prinzipien minimaler Berechtigungen an, hält Systeme und Applikationen aktuell, härtet exponierte Systeme und Dienste, schützt Secrets (Schlüssel, Token und Zertifikate) und organisiert deren Rotation.

Er konfiguriert Firewalls, segmentiert Netzwerke und filtert ein- und ausgehende Datenströme.

Sofern Backups nicht im Angebot enthalten sind, richtet er eigene Backups ein und testet regelmässig die Wiederherstellung.
Er überwacht die Nutzung seiner Ressourcen und reagiert unverzüglich auf Alarme oder Incidents.

6. E-Mail und kommerzielle Kommunikation

Der Kunde betreibt keine unzulässige Akquisition und unterlässt jede als SPAM einzustufende Praxis.

Er holt gültige und nachweisbare Einwilligungen ein (insbesondere mittels Double-Opt-in, wo angemessen), identifiziert sich klar als Absender, bietet einen sofortigen Abmeldemechanismus an und bewahrt die Nachweise auf.

Er implementiert SPF, DKIM und DMARC ordnungsgemäss und unterlässt den Kauf von Adressdatenbanken.

Die Dienste dürfen ohne vorherige schriftliche Genehmigung von HIDORA nicht als Plattform für den Massenversand verwendet werden.

7. Ressourcen, Leistung und Fair Use

Der Kunde respektiert die veröffentlichten Quoten, API-Limits, Service-Qualitätsparameter und Fair-Use-Regeln.

Absichtliche Überlastung oder Traffic-Inundation, die die Dienste beeinträchtigen könnten, ist verboten.

HIDORA kann verhältnismässige Massnahmen ergreifen, z. B. Rate-Limiting, Filtering, Netzwerk-Isolation, Blockierung von IPs oder Anwendung von Sicherheits-Patches, um Integrität und Verfügbarkeit der Umgebung sicherzustellen.

8. Personendaten und Persönlichkeitsrechte

Der Kunde stellt sicher, dass für alle Bearbeitungen von Personendaten eine Rechtsgrundlage besteht, informiert die betroffenen Personen gemäss dem anwendbaren Recht und hält das DSG und gegebenenfalls die DSGVO ein.

Inhalte, die Reputation, Bild, Stimme oder besonders schützenswerte Personendaten betreffen, werden nur auf rechtmässige, notwendige und verhältnismässige Weise bearbeitet.

Bei glaubhaften Vorwürfen einer Verletzung von Persönlichkeits- oder Urheberrechten findet das Notice-&-Action-Verfahren gemäss Anhang C Anwendung.

9. KI/ML und digitale Assets

Bei Training, Evaluation oder Nutzung von KI-Modellen mittels der Dienste hält der Kunde das anwendbare Recht strikt ein und bearbeitet keine Personendaten ohne entsprechende Rechtsgrundlage. Massives Sammeln oder Scraping von Drittdaten ohne Berechtigung ist untersagt.

Aktivitäten im Zusammenhang mit digitalen Assets (Mining, Staking, Masternodes) sind nur mit vorheriger schriftlicher Zustimmung von HIDORA und unter Berücksichtigung der technischen, elektrischen und thermischen Anforderungen sowie der Export- und Sanktionsregelungen zulässig.

10. Sicherheitstests und Responsible Disclosure

Penetrationstests oder aktive Scans erfordern die vorherige schriftliche Zustimmung von HIDORA, inkl. Umfang, Zeitfenster und Ursprungsadressen.

HIDORA unterstützt die verantwortungsvolle Meldung von Sicherheitslücken: Meldungen erfolgen vertraulich, ohne über verhältnismässige Proof-of-Concept-Nachweise hinaus zu agieren und ohne Zugriff auf, Veränderung oder Exfiltration von Drittdaten.

11. Missbrauchsmeldung und Kooperation

Missbrauch, Incidents oder Verdachtsfälle sind an abuse@hidora.io oder über das Support-Portal mit entsprechenden Belegen zu melden.

Der Kunde kooperiert nach Treu und Glauben mit HIDORA zur Eindämmung von Incidents, Durchführung der notwendigen Untersuchungen, Widerruf kompromittierter Secrets, Deployment von Patches und gegebenenfalls Vornahme der gesetzlich erforderlichen Meldungen.

HIDORA informiert den Kunden über Behördenanfragen, sofern dies gesetzlich zulässig und mit der Sicherheit der Umgebung vereinbar ist.

12. Durchsetzung und Korrekturmassnahmen

Bei tatsächlicher oder vermuteter Verletzung der AUP kann HIDORA unverzüglich verhältnismässige Massnahmen ergreifen, z. B. Isolation von Ressourcen, Blockierung von Datenflüssen, Einschränkung oder Sperrung bestimmter Funktionen.

Der Kunde wird informiert und, falls sinnvoll, ein Remediationsplan vorgeschlagen. Bei schwerwiegenden oder wiederholten Verstössen kann HIDORA die Dienste gemäss den AGB aussetzen oder kündigen.

Ist der Verstoss dem Kunden zuzurechnen, kann HIDORA die angemessenen Kosten für Untersuchung und Mitigation in Rechnung stellen.

13. Aufbewahrung und Löschung

HIDORA kann Logs und Aufzeichnungen zur Sicherheit, Abrechnung, Erfüllung gesetzlicher Verpflichtungen und Untersuchung von Incidents gemäss seiner Retention-Policy aufbewahren.

Löschung und gegebenenfalls Herausgabe von Daten erfolgen gemäss den AGB und Anhang D.

14. AUP-Updates

HIDORA kann die AUP aus rechtlichen, sicherheitsbezogenen oder technischen Gründen aktualisieren.

Änderungen werden veröffentlicht und gegebenenfalls dem Kunden mitgeteilt. Die fortgesetzte Nutzung der Dienste gilt als Annahme der aktualisierten Version.

15. Kontakt

Fragen zur AUP können an legal@hidora.io oder über das Support-Portal gerichtet werden.

Oktober 2025

Anhang B – Service Level Agreement (SLA)

1. Gegenstand und Geltungsbereich

Dieses SLA legt die verbindlichen Dienstverpflichtungen für die Cloud-Angebote (IaaS/PaaS) von HIDORA fest, die produktiv genutzt werden.

Es umfasst die Definition und Berechnung der Verfügbarkeit, Wartungsfenster, Messmethodik und Beweisvereinbarung, Ausschlüsse, Dienstgutschriften, Beantragungsverfahren sowie Support- und Reaktionszeitverpflichtungen. Beta/Preview-, Test- oder Evaluierungsumgebungen fallen nicht unter dieses SLA.

2. Definition der Verfügbarkeit und Messmethodik

«Verfügbarkeit» bezeichnet den Prozentsatz der Zeit innerhalb eines Kalendermonats, in dem die Steuerungsoberflächen und kritischen Komponenten eines Dienstes betriebsbereit sind und Anfragen gemäss den veröffentlichten Spezifikationen verarbeiten.

Die Messung erfolgt durch HIDORA mittels interner Sonden und Metriken, unter Ausschluss der in Artikel 6 genannten Fälle und ausserhalb angekündigter Wartungsfenster.

Ein Incident gilt als abgeschlossen, wenn die nominale Kapazität des Dienstes wiederhergestellt und durch die Überwachungssysteme validiert wurde. Systemprotokolle, Metriken und technische Aufzeichnungen von HIDORA gelten als Beweis, sofern der Kunde keine widersprüchlichen technischen Nachweise vorlegt.

3. Verfügbarkeitsverpflichtungen

HIDORA strebt eine hohe Verfügbarkeit an, angepasst an die jeweilige Natur des Dienstes. Zielwerte sind auf dem jeweiligen Service-Datenblatt veröffentlicht und können je nach vom Kunden eingesetzter Architektur variieren.

Bei Multi-Zonen- oder Multi-Node-Konfigurationen nach dokumentierten Best Practices hängt die tatsächliche Verfügbarkeit auch von der Applikationsarchitektur des Kunden, seiner Fehlertoleranz und Failover-Strategie ab.

4. Verfügbarkeitsziele

Die Verfügbarkeitsziele und die für jedes Angebot geltende Gutschriftenstaffel sind auf dem Service-Datenblatt veröffentlicht.

Im Falle eines Widerspruchs mit einer vertraglichen Anlage hat letztere Vorrang für die laufende Periode.

Änderungen werden mit einer Frist von mindestens dreissig (30) Tagen angekündigt und gelten nur für zukünftige Dienstzeiträume.

5. Wartungsfenster

Geplante Wartungsarbeiten erfolgen während der auf dem Portal/Service-Datenblatt veröffentlichten Wartungsfenster. HIDORA kündigt wesentliche Eingriffe vorher an. Notfallwartungen können ausserhalb der geplanten Fenster erfolgen, wenn sie zur

Behebung einer Sicherheitslücke oder eines Betriebsrisikos notwendig sind; HIDORA informiert dann mit möglichst angemessener Vorankündigung und erstellt nachträglich einen Bericht. Wenn möglich, werden Arbeiten so durchgeführt, dass sie keine oder minimale Auswirkungen haben. Kritische Sicherheitskorrekturen können ohne Vorankündigung erfolgen, wenn die Sicherheit oder Integrität der Umgebung dies erfordert.

6. Ausschlüsse

Nicht als Nichtverfügbarkeiten gelten: (a) angekündigte Wartungsfenster, (b) Ausfälle aufgrund von Komponenten, die nicht von HIDORA bereitgestellt wurden, oder aufgrund von Konfigurationen, die von Empfehlungen abweichen, (c) Incidents verursacht durch absichtliche Überlastung, Verstoss gegen die AUP oder Handlungen des Kunden/Dritter in seinem Auftrag, (d) höhere Gewalt, (e) Einschränkungen von Beta/Preview-Versionen, (f) Unterbrechungen aufgrund gesetzlicher Verpflichtungen, behördlicher Anordnungen oder Sicherheitsmassnahmen zum Schutz der Umgebung.

7. Dienstgutschriften und Beantragungsverfahren

Erfüllt ein Dienst innerhalb eines Kalendermonats das Verfügbarkeitsziel nicht, kann der Kunde eine Dienstgutschrift in Höhe eines Prozentsatzes der monatlichen Gebühren dieses Dienstes beantragen, gemäss der auf dem Service-Datenblatt veröffentlichten Gutschriftenstaffel.

Gutschriften sind keine Rückerstattungen, nicht auszahlbar und werden auf zukünftige Rechnungen angerechnet; sie stellen, soweit anwendbar, den ausschliesslichen Rechtsbehelf des Kunden für die im SLA abgedeckten Nichtverfügbarkeiten dar, unbeschadet der Haftungsbeschränkungen der AGB. Anträge müssen innerhalb von dreissig (30) Tagen nach Monatsende per Ticket über das Kundenportal gestellt werden und Incident, Datum/Uhrzeit, Auswirkungen und betroffene Ressourcen beschreiben. HIDORA prüft den Antrag anhand der eigenen Protokolle und informiert den Kunden mit Begründung. Wird die Frist oder das Verfahren nicht eingehalten, gilt der Antrag als verworfen.

8. Kundensupport und Reaktionszeiten

Der Kundensupport steht an Arbeitstagen, Montag bis Freitag, von 08:00 bis 18:00 Uhr (MEZ) über das Support-Portal (support.hidora.io) oder die E-Mail support@hidora.io zur Verfügung.

Die Infrastruktur wird rund um die Uhr überwacht und unterliegt einem Bereitschaftsdienst, um den operativen Betrieb sicherzustellen.

Reaktionszeiten richten sich nach der Schwere des Incidents:

- **Hohe Schwere:** max. 1 Stunde Betroffen sind Systemabstürze, Suspendierungen, Datenbeschädigung/-verlust oder Ausfall kritischer HIDORA-Funktionen ohne Umgehungsmöglichkeit. ;
- **Normale Schwere:** max. 2 Stunden Betroffen sind z. B. Systemneustarts, Recovery nach Fehlern, gravierende Leistungsprobleme oder eingeschränkter Betrieb ;
- **Geringe Schwere:** max. 8 Stunden Betroffen sind Incidents mit Umgehungsmöglichkeit, minimale Leistungsverschlechterungen oder funktionale/konfigurationsbezogene Supportanfragen.

Diese Reaktionszeiten sind operative Zielwerte; sofern nicht anders in den Besonderen Bedingungen vereinbart, stellen sie keine verbindliche Reparaturfrist dar.

9. SLA-Änderungen

HIDORA kann dieses SLA aus rechtlichen, technischen oder betrieblichen Gründen anpassen.

Änderungen werden veröffentlicht und gegebenenfalls dem Kunden mit angemessener Vorankündigung mitgeteilt. Änderungen der Verfügbarkeitsziele oder der Gutschriftenstaffel werden mindestens dreissig (30) Tage vorher angekündigt und gelten nur für zukünftige Dienstzeiträume.

Die fortgesetzte Nutzung der Dienste nach Inkrafttreten der Änderungen gilt als Annahme. Bereits erworbene Gutschriften für vergangene Zeiträume bleiben unberührt.

10. Prävalenz

Im Falle eines Widerspruchs zwischen diesem SLA und den Besonderen Bedingungen eines Dienstes haben die Besonderen Bedingungen Vorrang.

Bei Konflikten mit den AGB ist das SLA ergänzend auszulegen; Haftungsbeschränkungen und sonstige allgemeine Klauseln der AGB bleiben weiterhin anwendbar.

Anhang C – Verfahren «Notice & Action»
(Beeinträchtigung von Rechten und Persönlichkeit)

1. Gegenstand und Geltungsbereich

Diese Anlage beschreibt das von HIDORA eingerichtete Notice-&-Action-Verfahren, um Behauptungen von Rechtsverletzungen Dritter, die mittels der Dienste begangen wurden, sorgfältig und verhältnismässig zu behandeln.

Sie gilt insbesondere für Verletzungen des Persönlichkeitsrechts (einschliesslich Bild, Stimme und besonders schützenswerte Personendaten), Diffamierung, Verletzungen von Urheber- und Markenrechten sowie Verletzungen des Geschäftsgeheimnisses und allgemein für Inhalte, die nach schweizerischem Recht offensichtlich rechtswidrig sind.

2. Leitprinzipien

HIDORA handelt als Hosting-Anbieter und greift ohne Vorwegnahme der materiellen Streitfrage ein, wenn die Situation es erfordert, auf der Grundlage glaubwürdiger Elemente.

Das Eingreifen zielt darauf ab, einen schwerwiegenden Schaden zu verhindern oder einer gesetzlichen Verpflichtung oder einer Anordnung nachzukommen.

HIDORA sucht ein Gleichgewicht zwischen Meinungsfreiheit, Persönlichkeitsschutz und Rechten des geistigen Eigentums, unter Beachtung des Verhältnismässigkeitsprinzips.

3. Gültige Meldung

Eine Meldung gilt als gültig, wenn sie klar und vollständig enthält: (a) die genaue Identifizierung des strittigen Inhalts oder der strittigen Ressource (URL, Instanz-ID, relevanter Zeitstempel); (b) die Beschreibung der angeblich verletzten Rechte und die angerufene Rechtsgrundlage; (c) die relevanten Tatsachen und, wenn möglich, Beweismittel (Screenshots, Hash, Header-Auszug, WHOIS usw.); (d) die Kontaktangaben des Antragstellers (Name, Funktion, Adresse, E-Mail, Telefon) und gegebenenfalls den Nachweis der Vertretungsbefugnis; (e) eine Erklärung in gutem Glauben, die die Richtigkeit der Angaben und das Bestehen eines rechtlich geschützten Rechts oder Interesses bestätigt.

Meldungen sind an **legal@hidora.io** oder über das dafür vorgesehene Formular/Portal zu richten.

4. Eingangsbestätigung und Beurteilung

HIDORA bestätigt den Eingang unverzüglich, registriert die Meldung und nimmt eine summarische Plausibilitätsprüfung vor, die bei Bedarf durch Anfragen nach zusätzlichen Informationen beim Antragsteller ergänzt wird.

Ist die Meldung unvollständig, fordert HIDORA den Antragsteller auf, sie innerhalb einer angemessenen Frist zu vervollständigen. Andernfalls kann die Anfrage ohne weitere Bearbeitung geschlossen werden, unbeschadet einer neuen ordnungsgemäss vervollständigten Meldung.

5. Einstweilige Massnahmen

Erscheint die behauptete Verletzung offensichtlich oder wird eine Anordnung einer zuständigen Behörde mitgeteilt, kann HIDORA vorläufig und verhältnismässig eine oder mehrere der folgenden Massnahmen ergreifen: (i) gezieltes Entfernen oder Sperren des Inhalts; (ii) eingeschränkte Suspension eines Dienstes, eines Kontos oder einer Funktion; (iii) Filterung oder Zugangsbeschränkung nach Adressbereich, Region oder Protokoll; (iv) Aufforderung zur Korrekturmassnahme an den Kunden innert einer bestimmten Frist.

HIDORA benachrichtigt den betroffenen Kunden, soweit dies rechtlich möglich und mit der Sicherheit vereinbar ist, und lädt ihn ein, seine Stellungnahme einzureichen.

6. Gegennotifikation und Wiederherstellung

Der Kunde kann die Massnahmen anfechten, indem er innerhalb der angegebenen Frist eine begründete Gegennotifikation einreicht, begleitet von Belegen (z. B. Genehmigungen, Lizenzen, gesetzliche Ausnahmen, Wahrheit der Tatsachen, überwiegendes öffentliches Interesse).

HIDORA beurteilt die Situation dann im Lichte der widerstreitenden Elemente neu und kann gegebenenfalls den Inhalt wiederherstellen oder die Massnahmen anpassen. Bei einem fortbestehenden Streit über Rechts- oder Tatfragen kann HIDORA die Parteien einladen, die zuständige Behörde anzurufen; HIDORA hält sich an jede vollstreckbare Entscheidung oder Anordnung.

7. Beweissicherung und Zusammenarbeit

HIDORA kann die für Beweis-, Sicherheits- und Compliance-Zwecke unbedingt erforderlichen technischen Protokolle, Metadaten und Elemente für die notwendige Dauer aufbewahren.

Auf rechtsgültige Anfrage hin kooperiert HIDORA mit den zuständigen Behörden im Rahmen von Untersuchungen oder Verfahren, soweit dies das anwendbare Recht und die Sicherheit der Umgebung erlauben.

Zugangs- oder Offenlegungsanfragen müssen hinreichend präzise und rechtlich begründet sein.

8. Wiederholung und abgestufte Massnahmen

Bei wiederholten oder besonders schwerwiegenden Verstössen kann HIDORA abgestufte Massnahmen anwenden, die von der Verwarnung bis zur vorübergehenden Suspension oder gar zur Kündigung des Dienstes gemäss den AGB reichen.

HIDORA kann auch Remediationspflichten, Schulungen oder gezielte Audits auferlegen, wenn dies zur Verhinderung einer Wiederholung sinnvoll ist.

9. Verfahrensmissbrauch

Offensichtlich unbegründete, missbräuchliche oder bösgläubige Meldungen können abgewiesen werden.

HIDORA behält sich das Recht vor, Sicherheiten zu verlangen oder die angemessenen Analyse- und Bearbeitungskosten in Rechnung zu stellen, wenn der damit verbundene Aufwand offensichtlich das übersteigt, was von einem sorgfältigen Hosting-Anbieter erwartet werden kann, unbeschadet allfälliger Haftungsansprüche gegen den Urheber der missbräuchlichen Meldung.

10. Transparenz und Aktualisierung

HIDORA kann aggregierte und anonymisierte Informationen über das Volumen und die Typologie der bearbeiteten Meldungen veröffentlichen (Transparenzbericht), vorbehaltlich der Vertraulichkeits- und Sicherheitsanforderungen.

Diese Anlage kann aus rechtlichen, technischen oder betrieblichen Gründen aktualisiert werden. Änderungen werden veröffentlicht und gegebenenfalls dem Kunden mitgeteilt; die weitere Nutzung der Dienste gilt als Annahme.

11. Anwendbares Recht

Das vorstehend beschriebene Verfahren unterliegt schweizerischem Recht. Es gilt unbeschadet der Rechtswege vor den zuständigen Behörden oder Gerichten des im Vertrag bezeichneten Gerichtsstands.

Oktober 2025

Anhang D – Datenverarbeitungsvereinbarung (DPA – Subunternehmer)

1. Gegenstand, Parteien und Dauer

Diese Anlage regelt im Sinne des revidierten Bundesgesetzes über den Datenschutz (DSG) und gegebenenfalls der DSGVO die Bearbeitung von Personendaten durch HIDORA («Auftragsbearbeiter») im Auftrag des Kunden («Verantwortlicher») im Rahmen der Erbringung der Dienste.

Sie gilt für die Dauer des Vertrags und bis zur Erfüllung der nachstehend vorgesehenen Rückgabe- oder Löschungspflichten.

2. Datenkategorien, betroffene Personen und Verarbeitungszwecke

Sofern in den Besonderen Bedingungen nichts anderes vereinbart ist, können die Bearbeitungen Identifikations- und Kontaktdaten, technische Identifikatoren, Log- und Metadaten, applikative Inhalte, die der Kunde auf die Dienste lädt, sowie je nach Verwendung des Kunden Daten über seine eigenen Endkunden, Mitarbeitenden, Dienstleister und Interessenten umfassen.

Besonders schützenswerte Personendaten. Der Kunde wird darauf hingewiesen, dass die Dienste von HIDORA nicht spezifisch für die Bearbeitung von besonders schützenswerten Personendaten im Sinne des DSG oder gegebenenfalls besonderer Datenkategorien im Sinne der DSGVO (z. B. Gesundheitsdaten, biometrische oder genetische Daten, politische oder religiöse Ansichten, Daten über Straf- oder Sanktionsverfahren) bestimmt sind. Entscheidet der Kunde nach eigenem Ermessen dennoch, solche Daten mittels der Dienste zu bearbeiten, obliegt es ihm, die Rechtmässigkeit dieser Bearbeitung sicherzustellen, die betroffenen Personen zu informieren und die geeigneten technischen und organisatorischen Massnahmen zu treffen. HIDORA bearbeitet diese Daten unter denselben Sicherheitsbedingungen wie die übrigen Personendaten, kann jedoch nicht für das Fehlen spezifischer, vertraglich nicht vereinbarter Massnahmen verantwortlich gemacht werden.

Die Verarbeitungszwecke umfassen Hosting, Speicherung, Backup, Monitoring, Support und Wartung, Abrechnung, Sicherheit, Kontinuität und Verbesserung der Dienste, nur in dem Umfang, der für die Erfüllung des Vertrags erforderlich ist.

3. Rollen, Weisungen und Compliance

Der Kunde bestimmt die wesentlichen Zwecke und Mittel der Bearbeitung und bleibt allein verantwortlich für die Rechtmässigkeit der mittels der Dienste vorgenommenen Bearbeitungen.

HIDORA handelt ausschliesslich auf der Grundlage dokumentierter Weisungen des Kunden, einschliesslich für Übermittlungen in Drittländer, ausser bei zwingender gesetzlicher Verpflichtung; in diesem Fall informiert HIDORA den Kunden vor der Bearbeitung, soweit das anwendbare Recht dies erlaubt.

Der Kunde verpflichtet sich, nur rechtskonforme Weisungen zu erteilen und HIDORA unverzüglich über Änderungen zu informieren, die die Rechtmässigkeit der Bearbeitung beeinträchtigen könnten.

4. Vertraulichkeit und befugtes Personal

HIDORA stellt sicher, dass die zur Bearbeitung von Personendaten befugten Personen zur Vertraulichkeit verpflichtet sind und eine angemessene Schulung erhalten.

Die Berechtigungen werden nach dem Prinzip des «Need-to-know» erteilt und regelmässig überprüft. Jeder Zugriff wird verhältnismässig zu den Risiken protokolliert.

5. Technische und organisatorische Massnahmen (TOMs)

HIDORA trifft geeignete technische und organisatorische Massnahmen zur Risikominimierung, um ein angemessenes Sicherheitsniveau zu gewährleisten.

Diese Massnahmen umfassen insbesondere: Informationssicherheits-Governance, Identitäts- und Zugriffsmanagement (MFA wo anwendbar, Rollentrennung, Protokollierung), Netzwerkschutz (Segmentierung, Filterung, Monitoring), Datenschutz (Verschlüsselung ruhender und übertragener Daten wo relevant, Schlüsselzyklusmanagement), Schwachstellen- und Änderungsmanagement (Inventar, Patches, Reviews), Backup und regelmässige Wiederherstellungstests, Kontinuitäts- und Notfallpläne, Endgeräte- und Servermanagement (Härtung, Updates) sowie Betriebshygiene (Verfahren, Reviews, Sensibilisierung).

Auf angemessene Anfrage stellt HIDORA eine aktualisierte Beschreibung der TOM zur Verfügung.

6. Weitere Unterauftragsbearbeiter

HIDORA kann Weitere Unterauftragsbearbeiter für die Ausführung aller oder eines Teils der Bearbeitungen beiziehen.

HIDORA auferlegt diesen Dienstleistern gleichwertige Datenschutzpflichten wie die vorliegenden und bleibt dem Kunden gegenüber für die Handlungen und Unterlassungen dieser Unterauftragsbearbeiter verantwortlich.

HIDORA führt eine Liste der betreffenden Weiteren Unterauftragsbearbeiter und benachrichtigt den Kunden über jede wesentliche Änderung mit angemessener Vorankündigung. Der Kunde kann aus ernsthaften datenschutzrechtlichen Gründen einen begründeten Einwand erheben; die Parteien suchen nach Treu und Glauben eine zumutbare kommerzielle Lösung. Andernfalls kann der Kunde den betreffenden Dienstteil ohne Pönale ab Inkrafttreten der Änderung kündigen.

7. Lokalisierung und internationale Übermittlungen

Das Haupthosting erfolgt in der Schweiz, sofern nichts anderes vereinbart wurde. Wenn Nebenbearbeitungen eine Übermittlung in ein Land ohne anwendbaren Angemessenheitsentscheid erfordern, setzt HIDORA einen anerkannten Mechanismus ein (EU-Standardvertragsklauseln 2021, einschliesslich schweizerischem Addendum, oder gleichwertige Instrumente) und gegebenenfalls ergänzende Massnahmen im Sinne der Empfehlungen der zuständigen Behörden.

HIDORA prüft nach Treu und Glauben jedes Ersuchen des Kunden um zusätzliche Informationen zur Beurteilung der Übermittlungsrisiken.

8. Unterstützung des Verantwortlichen und Rechte betroffener Personen

HIDORA unterstützt den Kunden in angemessenem Umfang, soweit seine technischen und organisatorischen Möglichkeiten es erlauben, um ihm die Beantwortung von Rechtsausübungsanfragen zu ermöglichen, Datenschutz-Folgenabschätzungen durchzuführen und gegebenenfalls die Behörden oder betroffenen Personen zu benachrichtigen.

HIDORA leitet dem Kunden jede direkt von einer betroffenen Person erhaltene Anfrage weiter, ohne darauf zu antworten, ausser bei gegenteiliger Weisung oder gesetzlicher Verpflichtung.

9. Datenpannen und Incident-Management

HIDORA benachrichtigt den Kunden unverzüglich nach Kenntnisnahme eines Incidents, der Personendaten betrifft, die für den Kunden bearbeitet werden.

Die Meldung enthält die zu diesem Zeitpunkt verfügbaren Informationen und wird laufend ergänzt, insbesondere die Art des Incidents, die ungefähren Kategorien und Mengen betroffener Daten und Personen, die voraussichtlichen Folgen, die zur Behebung der Verletzung und zur Abschwächung ihrer Auswirkungen ergriffenen oder vorgeschlagenen Massnahmen sowie die relevanten Kontaktstellen. Der Kunde bleibt verantwortlich für die rechtliche Beurteilung der Verletzung und die Meldungen an die zuständigen Behörden oder betroffenen Personen gemäss dem anwendbaren Recht.

HIDORA nimmt ohne vorherige schriftliche Weisung des Kunden keine externe Meldung oder Kommunikation vor, ausser bei zwingender gegenteiliger gesetzlicher Verpflichtung. HIDORA dokumentiert jede Datenpanne, einschliesslich der damit zusammenhängenden Tatsachen, ihrer Auswirkungen und der ergriffenen Korrekturmassnahmen, um die Einhaltung der datenschutzrechtlichen Verpflichtungen nachzuweisen.

10. Unterstützung durch den Auftragsbearbeiter

HIDORA unterstützt den Kunden, soweit vernünftigerweise möglich und unter Berücksichtigung der Art der Bearbeitung sowie der ihr vorliegenden Informationen, um ihm die Erfüllung seiner Pflichten in den Bereichen Datensicherheit, Datenschutz-Folgenabschätzung und Vorabkonsultationen bei Aufsichtsbehörden zu ermöglichen.

HIDORA stellt dem Kunden die notwendigen Informationen zur Verfügung, um die Einhaltung der in dieser Vereinbarung vorgesehenen Pflichten nachzuweisen, und ermöglicht die Durchführung angemessener Audits gemäss den in den AGB vorgesehenen Bedingungen.

Jede von HIDORA in Anwendung dieses Artikels erbrachte Unterstützung, die über die gesetzlichen Mindestpflichten hinausgeht, kann zu einer zusätzlichen Vergütung auf der Basis des anwendbaren Stundensatzes führen.

11. Rückgabe und Löschung der Daten

Bei Ablauf oder Kündigung des Vertrags nimmt HIDORA gemäss den schriftlichen Weisungen des Kunden entweder die Rückgabe oder die endgültige Löschung sämtlicher für den Kunden bearbeiteten Personendaten vor, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

Die Löschung erfolgt auf sichere Weise gemäss den geltenden technischen Standards, die eine Wiederherstellung der Daten ausschliessen. HIDORA bestätigt dem Kunden die tatsächliche Durchführung dieser Löschung schriftlich.

Mangels spezifischer Weisung des Kunden innerhalb von dreissig (30) Tagen nach Vertragsende ist HIDORA zur Löschung berechtigt; diese erfolgt spätestens innerhalb der darauffolgenden dreissig (30) Tage (ausser gesetzliche Aufbewahrungspflichten). Auf vorherige Anfrage des Kunden kann eine Rückgabe in einem angemessenen Standardformat organisiert werden; hierfür können Gebühren anfallen.

12. Internationale Datenübermittlungen

Das Haupthosting erfolgt in der Schweiz.

Damit verbundene Bearbeitungen (z. B. Anti-DDoS, Monitoring, Support, Backups) können Weitere Unterauftragsbearbeiter einbeziehen. Jede Übermittlung ausserhalb der Schweiz/des EWR stützt sich auf einen anerkannten Mechanismus (insbesondere EU-Standardvertragsklauseln ergänzt durch das schweizerische Addendum oder einen Angemessenheitsentscheid), verbunden mit geeigneten ergänzenden Massnahmen.

HIDORA stellt sicher, dass jeder betreffende Weitere Unterauftragsbearbeiter ein dem anwendbaren schweizerischen und europäischen Recht gleichwertiges Schutzniveau bietet.

13. Anwendbares Recht und zuständige Gerichtsbarkeit

Diese Vereinbarung unterliegt schweizerischem Recht, unter Ausschluss seiner Kollisionsnormen und jeglicher internationaler Übereinkommen über den Warenkauf.

Jede Streitigkeit über die Gültigkeit, Auslegung oder Erfüllung dieser Vereinbarung unterliegt der ausschliesslichen Zuständigkeit der Gerichte am Sitz der HIDORA SA, vorbehaltlich zwingender Rechtswege.

Oktober 2025

Anhang E – Vertraulichkeit (NDA Framework)

1. Gegenstand und Geltungsbereich

Diese Anlage regelt die Vertraulichkeit ausserhalb von Personendaten (letztere bleiben durch Anhang D – Datenverarbeitungsvertrag geregelt). Sie gilt für alle vertraulichen Informationen, die zwischen den Parteien im Rahmen des Vertrags ausgetauscht werden, einschliesslich vorvertraglicher und unmittelbarer nachvertraglicher Austausche.

2. Definitionen

Jede nicht öffentliche Information, in jeder Form (schriftlich, mündlich, visuell, Code, Konfigurationen, Schemata, Metriken, Protokolle, Know-how, Geschäftspläne, Preisgestaltung), die als vertraulich gekennzeichnet oder vernünftigerweise als vertraulich erkennbar ist und von einer Partei (der «**Offenlegenden Partei**») an die andere (die «**Empfangende Partei**») übermittelt wird.

Nicht vertraulich sind Informationen, die: (i) ohne Verschulden der Empfangenden Partei öffentlich geworden sind; (ii) rechtmässig von einem nicht zur Vertraulichkeit verpflichteten Dritten erhalten wurden; (iii) unabhängig entwickelt wurden; (iv) der Empfangenden Partei bereits ohne Vertraulichkeitsverpflichtung bekannt waren.

3. Zulässige Verwendung

Die Empfangende Partei verwendet die vertraulichen Informationen ausschliesslich zur Vertragserfüllung und unterlässt jede andere Verwertung, direkt oder indirekt. Jede Kopie oder Extraktion muss strikt auf diesen Zweck beschränkt bleiben.

4. Eingeschränkter Zugang

Die Empfangende Partei beschränkt den Zugang auf Personen mit einem «Need-to-know» (Personal, Beauftragte, Unterbeauftragte, Berater, zusammen die «Berechtigten Personen/Covered Persons»), die einer gleichwertigen Vertraulichkeitsverpflichtung unterliegen. Die Empfangende Partei bleibt für Verstösse dieser Personen verantwortlich.

5. Schutzmassnahmen

Die Empfangende Partei trifft geeignete technische und organisatorische Massnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen, mindestens auf einem Niveau, das dem für ihre eigenen sensiblen Informationen angewandten entspricht, im Einklang mit den bewährten Praktiken der Branche. Protokolle, Metriken und technische Aufzeichnungen können gemäss dem Vertrag zu Beweis- und Sicherheitszwecken aufbewahrt werden.

6. Obligatorische Offenlegungen

Wenn das Gesetz, eine Anordnung oder eine zuständige Behörde eine Offenlegung vorschreibt, kann die Empfangende Partei den strikt notwendigen Teil mitteilen, nach vorheriger Benachrichtigung der Offenlegenden Partei (sofern gesetzlich zulässig), um ihr die Möglichkeit zu geben zu handeln, und unter Beantragung geeigneter Schutzmassnahmen (Siegelung, Ausschluss der Öffentlichkeit, Protective Order).

7. Vertraulichkeits-Incidents

Die Empfangende Partei informiert die Offenlegende Partei unverzüglich über jeden ihr bekannt gewordenen unbefugten Zugang zu vertraulichen Informationen und kooperiert nach Treu und Glauben zur Begrenzung der Auswirkungen. Betrifft der Incident Personendaten, gelten die Pflichten und Fristen von Anhang D.

8. Rückgabe und Vernichtung

Auf erstes Verlangen der Offenlegenden Partei oder bei Vertragsende gibt die Empfangende Partei die vertraulichen Informationen zurück oder vernichtet sie (einschliesslich Kopien, Notizen, Ableitungen), vorbehaltlich: (i) der standardmässigen technischen Backups und Aufbewahrungen; (ii) der gesetzlichen Aufbewahrungspflichten; und (iii) der zu Beweis-, Sicherheits- und Compliance-Zwecken aufbewahrten Elemente. Die Empfangende Partei bestätigt die Vernichtung auf angemessene Anfrage.

9. Residualwissen

Die Verwendung allgemeiner Kompetenzen, Ideen oder Know-hows, die durch das blosse Funktionieren des Gedächtnisses der Personen der Empfangenden Partei zurückbehalten werden, ist nicht eingeschränkt, sofern keine vertraulichen Informationen offengelegt oder Rechte des geistigen Eigentums verletzt werden.

10. Dauer

Sofern kein spezifisches NDA zwischen den Parteien strengere Bestimmungen vorsieht, gelten die Pflichten dieser Anlage auf unbestimmte Zeit, solange die Informationen nicht in die Öffentlichkeit gelangen; Geschäftsgeheimnisse bleiben unbefristet geschützt.

11. Vorrang und Verhältnis

Im Falle eines Konflikts zwischen dieser Anlage und einem spezifischen NDA, das für einen bestimmten Gegenstand oder ein bestimmtes Projekt abgeschlossen wurde, hat das spezifische NDA für dieses Projekt/diesen Gegenstand Vorrang.

Im Falle eines Konflikts zwischen dieser Anlage und den AGB hat Anhang E für die Vertraulichkeit ausserhalb von Personendaten Vorrang (letztere fallen unter Anhang D).

12. Anwendbares Recht

Diese Anlage unterliegt schweizerischem Recht; ausschliesslicher Gerichtsstand ist Genf, gemäss dem Artikel «Anwendbares Recht und Gerichtsstand» des Vertrags.

Oktober 2025