AMNIS API ALLGEMEINE GESCHÄFTSBEDINGUNGEN (AGB)

Version 1.1 / 15.09.2025

Einführung

Diese Vereinbarung über die Allgemeinen Geschäftsbedingungen für API („Vereinbarung“) wird zwischen der Amnis Europe AG, einem regulierten und lizenzierten Zahlungsinstitut unter der Aufsicht der Liechtensteiner Finanzmarktaufsicht (FMA) mit Sitz in Gewerbeweg 15, 9490 Vaduz, Liechtenstein (nachfolgend ‚amnis'), und dem Kunden (nachfolgend „Kunde“), wie unten definiert, geschlossen.

Definitionen

„API“	bezeichnet die von amnis bereitgestellte(n) Anwendungsprogrammierschnittstelle(n), Entwickler-Tools, Dokumentation und zugehörige Technologie für den Zugang zu bestimmten Funktionen und Diensten, einschließlich, aber nicht beschränkt auf Kartenausstellung, Kontostandsprüfung, Abgleich und Berichterstattung. In der aktuellen Version sind Zahlungseinleitung und Devisengeschäfte nicht über die API verfügbar.
„Kunde“	bezieht sich auf die juristische Person, die sich für die API registriert oder diese nutzt, entweder direkt oder durch autorisiertes Personal. Dazu gehören alle Unternehmen oder Dienstleistungsanbieter, wie z. B. eine Spesenmanagement-Plattform, ein ERP-System oder eine Treasury-Plattform, in die amnis-Dienste integriert werden, um ihren eigenen Endnutzern Funktionen anzubieten (zusammenfassend als „Anbieter“ bezeichnet).
„Endnutzer“	bezeichnet natürliche oder juristische Personen, die Dienstleistungen vom Kunden (einschließlich Anbietern) über die Integration des Kunden mit amnis erhalten. Endnutzer können zum Beispiel virtuelle oder physische Karten anfordern oder über eine Client-Anwendung, die eine Schnittstelle zur amnis-API hat, auf Guthaben- und Transaktionsdaten zugreifen.
„Vertrauliche Informationen“	umfasst alle nicht öffentlichen technischen, finanziellen oder betrieblichen Informationen, die zwischen den Parteien ausgetauscht werden, unabhängig davon, ob sie mündlich, schriftlich, digital oder anderweitig aufgezeichnet wurden, und die eine vernünftige Person als vertraulich ansehen würde.
„Transaktionsdaten“	umfasst alle Daten im Zusammenhang mit der Nutzung der API, einschließlich Kartenanfragen, Autorisierungen, Abrechnungsbestätigungen, Saldeninformationen und zugehörige Metadaten.
„Schreibgeschützter Zugriff“	bezeichnet einen API-Zugang, der es dem Kunden ermöglicht, Daten wie Kontostände, Transaktionshistorien und Karten-Metadaten abzurufen, anzuzeigen oder darüber zu berichten, ohne dass er in der Lage ist, Finanztransaktionen zu initiieren, Kontoinformationen zu ändern oder einen Systemzustand zu verändern.
„Lese- und Schreibzugriff“	bedeutet API-Zugang, der es dem Kunden ermöglicht, sowohl Datenabfragen als auch autorisierte Transaktionseinleitungs-

	oder -änderungsfunktionen durchzuführen, einschließlich, aber nicht beschränkt auf: • Zahlungen: Initiierung von ausgehenden Banküberweisungen oder Geldtransfers. • Ausstellung von Karten: Beantragung der Ausstellung oder Entwertung von physischen oder virtuellen Karten. • FX: Übermittlung von Instruktionen zum Umtausch von Währungen oder zur grenzüberschreitenden Abwicklung.
„Plattformanbieter“	bezeichnet einen Kunden, der die amnis-API in seine eigene Softwareplattform, sein Portal oder sein Produkt integriert, um amnis-fähige Dienste für nachgeschaltete Endnutzer wie Geschäftskunden oder Anwendungsnutzer anzubieten.

1 LIZENZERTEILUNG UND BESCHRÄNKUNGEN

1.1. amnis gewährt dem Kunden eine nicht ausschließliche, nicht übertragbare, widerrufliche Lizenz für den Zugriff auf die API und deren Nutzung ausschließlich für legitime interne Geschäftszwecke, vorbehaltlich dieses Vertrags.

1.2. Der Kunde darf

- die API nicht rückentwickeln, kopieren, verändern oder modifizieren,
- die API nicht für ungesetzliche, riskante oder verbotene Aktivitäten nutzen,
- keinem unbefugten Dritten den Zugriff auf die API ermöglichen,
- die Sicherheit der amnis-Plattform oder der Zugangsbeschränkungen nicht verletzen.

2 VERANTWORTLICHKEITEN DES KUNDEN

2.1 Der Kunde muss

- die Sicherheitsmaßnahmen auf dem neuesten Stand halten, einschließlich der Multi-Faktor-Authentifizierung (2FA), um Zahlungen einzuleiten, Karten auszugeben oder Kartendaten (z. B. PIN-Codes) zu erhalten,
- die Ausgabe von API-Schlüsseln auf autorisiertes Personal beschränken,
- eine angemessene Authentifizierung von Endbenutzern sicherstellen, eine entsprechende Zustimmung der Endbenutzer einholen und Missbrauch verhindern,
- in Übereinstimmung mit den geltenden Gesetzen operieren,
- amnis unverzüglich, spätestens jedoch innerhalb von 24 Stunden, über jede Sicherheitsverletzung oder verdächtige API-Aktivität informieren.
- Der Kunde muss die Protokollierung aller API-Aktivitäten implementieren und aufrechterhalten, ausreichend zur Unterstützung von Sicherheitsüberwachung, Vorfalluntersuchungen und Prüfbarkeit, unabhängig vom Zugriffstyp. Wenn die Aufbewahrung von Protokolldaten nicht möglich ist oder im Falle eines Streits, einer Untersuchung oder eines Vorfalls der Kunde keine gültigen Protokolldaten zur Unterstützung seiner Position bereitstellen kann, erkennt der Kunde an, dass amnis für den betreffenden Vorfall keine Haftung übernimmt.
- Basierend auf der Zugangsart:
    - Nur Lesezugriff:
        - alle API-Datenabrufe protokollieren,
        - die abgerufenen Daten bei der Übertragung und im Ruhemodus verschlüsseln,
        - die Datenpersistenz begrenzen, Speicherungskontrollen anwenden

- Lesen und Schreiben:
  - Zahlungen – Implementierung von Transaktionsauthentifizierung und Prüfpfaden.
  - Kartenausgabe – Zugriff beschränken, Kontrollen bei der Kartenerstellung durchführen und eine starke Kundenauthentifizierung implementieren.
  - FX – Die Vertragsparteien bestätigen das Devisen-Testprotokoll (FX).
- Plattform-Anbieter:
  - Trennung der Kundendaten einhalten,
  - auf Anfrage Prüfungsnachweise vorlegen,
  - den nachgeordneten Zugang bei Bedarf widerrufen.

3 DATENSCHUTZ UND SICHERHEIT

3.1 Beide Parteien verpflichten sich zur Einhaltung der geltenden Datenschutzgesetze, einschließlich der Datenschutz-Grundverordnung (DSGVO) und des liechtensteinischen Datenschutzgesetzes.

3.2 Der Kunde darf

- Transaktions- und personenbezogene Daten nur für rechtmäßige Zwecke speichern,
- muss die Verschlüsselung von Daten bei der Übertragung und im Ruhezustand sicherstellen,
- die Nutzung der Daten auf rechtmäßige Zwecke beschränken,
- den unbefugten Export und die unbefugte Nutzung von Daten verhindern,
- darf keine personenbezogenen Daten ohne rechtmäßige Grundlage in Länder außerhalb des EWR exportieren.

3.3 amnis behält sich das Recht vor, API-Implementierungen auf Konformität und Sicherheit zu prüfen.

3.4 Der Zugriff auf die amnis API muss jederzeit geeigneten Maßnahmen zum Datenzugriff und -schutz unterliegen. Mindestens muss der Kunde für alle Konten oder Systeme, die amnis API-Zugangsdaten enthalten oder verwenden, eine Multi-Faktor-Authentifizierung (MFA) durchsetzen. MFA kann zeitbasierte Einmalpasswörter, Push-Benachrichtigungen oder Hardware-Token umfassen. amnis kann die Einführung stärkerer Authentifizierungsmethoden (z. B. phishing-resistente MFA) empfehlen oder verlangen, wenn dies zur Einhaltung sich entwickelnder regulatorischer oder sicherheitsrelevanter Standards erforderlich ist. Das Versäumnis, MFA mindestens auf diesem Niveau aufrechtzuerhalten, führt dazu, dass der Kunde die volle Verantwortung für alle daraus resultierenden Verstöße oder Missbräuche übernimmt.

4 GEBÜHREN

4.1 Derzeit erhebt amnis keine gesonderten Gebühren für die API-Nutzung. Den Kunden entstehen nur Kosten im Zusammenhang mit den zugrundeliegenden Diensten, auf die über die API zugegriffen wird (z. B. Kartenausgabe oder Abrechnungsdienste), die durch die geltenden Produktpreise geregelt sind.

4.2 amnis behält sich das Recht vor, in Zukunft API-spezifische Gebühren einzuführen, direkt oder gekoppelt an die Nutzung der amnis-Basisplattform. Jede derartige Änderung wird im Voraus mitgeteilt und in einer geänderten Gebührenordnung berücksichtigt, die mindestens 60 Tage im Voraus schriftlich angekündigt werden muss.

4.3 Die Einführung künftiger API-Nutzungsgebühren muss so gestaltet sein, dass Transparenz und Fairness gewährleistet sind, insbesondere bei großvolumigen oder kommerziellen Integrationen, ohne den grundlegenden Zugang zu den amnis-Diensten zu behindern.

5 RATENBESCHRÄNKUNGEN

5.1 Die amnis-API unterliegt bestimmten Ratenbeschränkungen, um die Stabilität und Leistung der Plattform zu gewährleisten. Die Kunden müssen sich an die in der API-Dokumentation angegebene Höchstzahl der zulässigen Anfragen pro Endpunkt halten.

5.2 Überschreitet der Kunde die Ratenbeschränkung, können Anfragen gedrosselt oder vorübergehend abgewiesen werden. Bei fortgesetzter Nichteinhaltung können der Zugang eingeschränkt oder die API-Zugangsdaten gesperrt werden.

5.3 amnis behält sich das Recht vor, die Ratenbeschränkungen mit Vorankündigung anzupassen und wird alle Änderungen auf dem Entwicklerportal veröffentlichen.

6 API-VERSIONIERUNG UND -VERALTUNG

6.1 amnis arbeitet mit versionierten APIs. Die aktuell verwendete Version wird im Entwicklerportal dokumentiert.

6.2 Falls eine veraltete Version der API ausgetauscht werden soll, wird amnis dies mindestens 90 Tage im Voraus ankündigen. Veraltete Versionen können für eine begrenzte Zeit unterstützt werden, um einen reibungslosen Übergang zu gewährleisten.

6.3 Die Kunden sind für die rechtzeitige Migration auf unterstützte API-Versionen verantwortlich.

7 VERFAHREN ZUR MITTEILUNG VON ÄNDERUNGEN

7.1 amnis kann die API, die Dokumentation oder die Allgemeinen Geschäftsbedingungen von Zeit zu Zeit aktualisieren. Wesentliche Änderungen werden mindestens 30 Tage im Voraus über das Entwicklerportal oder die registrierte Kontakt-E-Mail-Adresse bekannt gegeben.

7.2 Geringfügige oder nicht funktionsrelevante Änderungen (z. B. Fehlerbehebungen, interne Verbesserungen) können ohne förmliche Mitteilung vorgenommen werden.

7.3 Kunden wird empfohlen, den API-Changelog-Feed zu abonnieren, um über laufende Aktualisierungen informiert zu werden.

8 DIENSTLEISTUNGSVEREINBARUNG („SERVICE LEVEL AGREEMENT", SLA)

8.1 amnis unternimmt wirtschaftlich vertretbare Anstrengungen, um die monatlich erfasste API-Verfügbarkeit von 99,9 % aufrechtzuerhalten, ausgenommen geplante Wartungsarbeiten.

8.2 Geplante Wartungsfenster werden mindestens 48 Stunden im Voraus veröffentlicht und, wenn möglich, außerhalb der Hauptgeschäftszeiten durchgeführt.

8.3 amnis reagiert auf kritische API-Vorfälle, die über den vorgesehenen Support-Kanal gemeldet werden, innerhalb von einer Geschäftsstunde und stellt danach Updates bereit, bis sie gelöst sind.

8.4 Diese SLA gilt nicht für Störungen, die durch Faktoren verursacht werden, die außerhalb der Kontrolle von amnis liegen, wie z. B. durch Fremdverschulden oder Ereignisse höherer Gewalt.

9 DATENVERARBEITUNGSVEREINBARUNG („DATA PROCESSING AGREEMENT", DPA)

9.1 Für die Zwecke der DSGVO und anderer anwendbarer Datenschutzgesetze fungiert amnis als Datenverarbeiter und der Kunde als Datenverantwortlicher für die über die API verarbeiteten personenbezogenen Daten.

9.2 amnis darf/muss:

- personenbezogene Daten nur auf dokumentierte Anweisung des Auftraggebers verarbeiten,
- geeignete technische und organisatorische Sicherheitsmaßnahmen umsetzen,
- sicherstellen, dass die zur Verarbeitung personenbezogener Daten befugten Mitarbeiter zur Vertraulichkeit verpflichtet sind,
- den Kunden bei der Beantwortung von Auskunftsersuchen Betroffener und behördlichen Anfragen unterstützen,
- den Kunden unverzüglich benachrichtigen, wenn er von einer Verletzung des Datenschutzes in Bezug auf personenbezogene Daten erfährt.

9.3 Der Kunde gewährleistet, dass er über eine rechtmäßige Grundlage für die Verarbeitung der über die API übermittelten personenbezogenen Daten verfügt und dass er alle Datenschutzverpflichtungen einhält, die für Datenverantwortliche gelten.

10 LAUFZEIT UND KÜNDIGUNG

10.1 Dieses Abkommen bleibt in Kraft, bis es von einer der Parteien mit einer Frist von 30 Tagen schriftlich gekündigt wird.

10.2 amnis kann den API-Zugang sofort aussetzen oder widerrufen:

- im Falle der Nichteinhaltung dieses Abkommens,
- aufgrund einer bestätigten oder vermuteten Datenschutzverletzung.
- infolge von Anweisungen der Regulierungsbehörden.

10.3 Nach der Kündigung muss der Kunde:

- den Zugriff auf und die Nutzung der API einstellen,
- alle vertraulichen Informationen vernichten oder zurückgeben,

- die Löschung aller von der API stammenden Daten nachweisen.

11 GEISTIGES EIGENTUM

11.1 Alle Rechte, Titel und Ansprüche an der API, der Dokumentation und den Plattformtechnologien bleiben das ausschließliche Eigentum von amnis.

11.2 Dem Kunden werden keine Rechte an geistigem Eigentum eingeräumt, es sei denn, dies ist in diesem Vertrag ausdrücklich vorgesehen.

12 HAFTUNGSBESCHRÄNKUNG

12.1 Keine der Parteien haftet für indirekte, zufällige oder Folgeschäden, einschließlich entgangener Gewinne, Datenverluste oder Rufschädigung.

12.2 Die kumulative Gesamthaftung von amnis im Rahmen dieses Vertrags übersteigt nicht den Gesamtbetrag der API-Gebühren, die der Kunde in den 12 Monaten vor dem Ereignis, das den Anspruch begründet, gezahlt hat, es sei denn, sie wurde durch grobe Fahrlässigkeit, vorsätzliches Fehlverhalten oder eine Verletzung der Vorschriften seitens amnis verursacht.

12.3 Der Kunde übernimmt die volle Haftung für jede Datenschutzverletzung, die sich aus dem Versäumnis ergibt, die erforderlichen Mindestkontrollen für die API-Sicherheit zu implementieren, einschließlich, aber nicht beschränkt auf 2FA, Rotation der Anmeldeinformationen und Ratenbeschränkung.

13 ENTSCHÄDIGUNG

13.1 Der Kunde verpflichtet sich, amnis von allen Ansprüchen, Schäden und Verlusten freizustellen, die sich aus folgenden Gründen ergeben:

- Verstöße gegen geltende Gesetze oder Vorschriften,
- unbefugter API-Zugriff aufgrund von Nachlässigkeit auf Kundenseite,
- Ansprüche von Endnutzern im Zusammenhang mit den Dienstleistungen des Kunden oder der Datenverarbeitung.

13.2 amnis wird im Falle einer Inanspruchnahme durch einen Dritten in angemessener Weise kooperieren und diesen informieren.

14 GELTENDES RECHT UND STREITBEILEGUNG

14.1 Dieser Vertrag unterliegt ausschließlich dem Recht Liechtensteins, ohne Rücksicht auf kollisionsrechtliche Grundsätze.

14.2 Alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag ergeben, werden durch ein Schiedsverfahren mit Sitz in Vaduz, Liechtenstein, in englischer Sprache gemäß der Schiedsgerichtsordnung der Liechtensteinischen Schiedsgerichtsvereinigung beigelegt. Die Entscheidung des Schiedsgerichts ist endgültig und verbindlich.

15 VERSCHIEDENES

15.1 Diese Vereinbarung stellt die vollständige Vereinbarung zwischen den Parteien in Bezug auf die API dar.

15.2 Änderungen bedürfen der Schriftform und der Unterschrift eines Bevollmächtigten.

15.3 Der Kunde darf diesen Vertrag nicht ohne vorherige schriftliche Zustimmung von amnis abtreten.

15.4 Sollte sich eine Bestimmung als nicht durchsetzbar erweisen, so bleibt der Rest der Vereinbarung in Kraft.

15.5 Die Abschnitte über die Vertraulichkeit, den Umgang mit Daten, die Haftung und die Beilegung von Streitigkeiten gelten auch nach der Kündigung.