AMNIS API

TERMS AND CONDITIONS (T&Cs)

Version 1.1 / 15.9.2025

Introduction

This API Terms and Conditions Agreement ("Agreement") is entered into by and between Amnis Europe AG, a regulated and licensed payment institution, under the supervision of the Liechtenstein Financial Market Authority (FMA), with its principal office at Gewerbeweg 15, 9490 Vaduz, Liechtenstein (hereafter "amnis"), and the Client (hereafter "Client"), as defined below.

Definitions

“API”
means the application programming interface(s), developer tools, documentation, and related technology provided by amnis for access to certain features and services, including but not limited to card issuance, account balance checks, reconciliation, and reporting. For the current version, payment initiation and foreign exchange operations are not available via the API.

“Client”
refers to the legal entity that registers for or uses the API, either directly or through authorized personnel. This includes any business or service provider, such as an expense management platform, ERP system, or treasury platform, that integrates with amnis services to offer functionality to their own end users (collectively referred to as "Providers").

“End User”
means individuals or entities receiving services from the Client (including Providers) via the Client's integration with amnis. End Users may, for example, request virtual or physical cards or access balance and transaction data through a Client application that interfaces with the amnis API.

“Confidential Information”
includes any non-public technical, financial, or operational information exchanged between the parties, whether oral, written, digital, or otherwise recorded, that a reasonable person would consider confidential.

“Transaction Data”
includes all data related to usage of the API, including card requests, authorizations, settlement confirmations, balance information, and related metadata.

“Read-only Access”
means API access that permits the Client to retrieve, view, or report on data such as account balances, transaction histories, and card metadata, without the ability to initiate financial transactions, modify account information, or alter any system state.

“Read & Write Access”
means API access that enables the Client to perform both data retrieval and authorized transaction initiation or modification functions, including but not limited to:

- Payments: Initiating outbound bank wires or fund transfers.
- Card Issuance: Requesting issuance or cancellation of physical or virtual cards.
- FX: Submitting instructions to exchange currencies or trigger cross-border settlement.

“Platform Provider” means a Client that integrates the amnis API into its own software platform, portal, or product to offer amnis-enabled services to downstream End Users, such as business customers or application users.

1 LICENSE GRANT & RESTRICTIONS

1.1. amnis grants the Client a non-exclusive, non-transferable, revocable license to access and use the API solely for legitimate internal business purposes, subject to this Agreement.

1.2. The Client shall:

- Not reverse engineer, copy, alter or modify the API.
- Not use the API for unlawful, high-risk, or prohibited activities.
- Not permit any unauthorized third party to access the API.
- Not breach amnis' platform security or access restrictions.

2 CLIENT RESPONSIBILITIES

2.1 The Client must:

- Maintain up-to-date security controls, including multi-factor authentication (2FA) to initiate payments, issue cards, or receive card details (e.g. PIN code).
- Limit API key distribution to authorized personnel.
- Ensure appropriate End User authentication, obtain appropriate End User consent, and prevent misuse.
- Operate in compliance with applicable laws.
- Notify amnis immediately and within no more than 24 hours of any security breach or suspicious API activity.
- The Client shall implement and maintain logging of all API activity sufficient to support security monitoring, incident investigation, and auditability, regardless of access type. Where retention of logging data is not possible, or if a dispute, investigation, or incident arises and the Client cannot provide valid log data to support its position, the Client acknowledges that amnis shall bear no liability for the incident in question.
- Based on Access Type:
    - Read-only Access:
        - Encrypt retrieved data in transit and at rest.
        - Limit data persistence; apply retention controls.
    - Read & Write:
        - Payments – Implement transactional authentication and audit trails.

        - Card Issuance – Limit access, enforce card creation controls, and implement strong customer authentication.
        - FX – Parties shall confirm the foreign exchange (FX) test protocol.
    - Platform Providers
        - Maintain tenant data segregation.
        - Provide audit evidence upon request.
        - Revoke downstream access on demand.

3 DATA PRIVACY & SECURITY

3.1 Both parties agree to comply with applicable data protection laws, including the General Data Protection Regulation (GDPR) and Liechtenstein Data Protection Act.

3.2 The Client shall:

- Only retain transactional and personal data for lawful purposes.
- Ensure encryption of data in transit and at rest.
- Limit data use to lawful purposes.
- Avoid unauthorized data export and usage.
- Not export personal data outside the EEA without lawful basis.

3.3 amnis reserves the right to audit API implementations for compliance and security.

3.4 Access to the amnis API must at all times be subject to appropriate data access and protection measures. At a minimum, the Client shall enforce multi-factor authentication (MFA) for all accounts or systems that hold or use amnis API credentials. MFA may include time-based one-time passwords, push notifications, or hardware tokens. amnis may recommend or require the adoption of stronger authentication methods (such as phishing-resistant MFA) where necessary to meet evolving regulatory or security standards. Failure to maintain MFA at this minimum level will result in the Client assuming full liability for any resulting breach or misuse.

4 FEES

4.1 At present, amnis does not charge any separate fees for API usage. Clients will only incur costs associated with underlying services accessed via the API (e.g., card issuance or settlement services), which are governed by applicable product pricing.

4.2 amnis reserves the right to introduce API-specific fees in the future, directly or bundled with core amnis platform usage. Any such change will be communicated in advance and reflected in a revised Fee Schedule, subject to a minimum of 60 days' prior written notice.

4.3 The introduction of future API usage charges shall be designed to ensure transparency and fairness, particularly for high-volume or commercial integrations, without hindering baseline access to amnis services.

5 RATE LIMITS

5.1 The amnis API is governed by defined rate limits to maintain platform stability and performance. Clients shall adhere to the maximum number of allowed requests per endpoint as outlined in the API documentation.

5.2 If the Client exceeds the rate limit, requests may be throttled or temporarily rejected. Continued non-compliance may result in restricted access or suspension of API credentials.

5.3 amnis reserves the right to adjust rate limits with advance notice and will publish any changes on the developer portal.

6 API VERSIONING & DEPRECATION

6.1 amnis maintains versioned APIs. The current version in use will be documented on the developer portal.

6.2 In the event of planned API deprecation, amnis will provide at least 90 days' notice. Deprecated versions may be supported for a limited time to ensure a smooth transition.

6.3 Clients are responsible for timely migration to supported API versions.

7 CHANGE NOTIFICATION PROCEDURE

7.1 amnis may update the API, documentation, or terms from time to time. Material changes will be communicated at least 30 days in advance via the developer portal or registered contact email.

7.2 Minor or non-functional changes (e.g., bug fixes, internal enhancements) may be made without formal notification.

7.3 Clients are encouraged to subscribe to the API changelog feed to stay informed of ongoing updates.

8 SERVICE LEVEL AGREEMENT (SLA)

8.1 amnis will use commercially reasonable efforts to maintain API uptime of 99.9% measured monthly, excluding scheduled maintenance.

8.2 Scheduled maintenance windows will be published at least 48 hours in advance and, where possible, conducted during non-peak hours.

8.3 amnis will respond to critical API incidents reported via the designated support channel within 1 business hour, with updates provided thereafter until resolved.

8.4 This SLA does not apply to interruptions caused by factors outside of amnis' control, such as third-party failures or force majeure events.

9 DATA PROCESSING AGREEMENT (DPA)

9.1 For the purposes of GDPR and other applicable privacy laws, amnis acts as a data processor and the Client as a data controller for personal data processed via the API.

9.2 amnis shall:

- Process personal data only on documented instructions from the Client.
- Implement appropriate technical and organizational security measures.
- Ensure that personnel authorized to process personal data are bound by confidentiality obligations.
- Assist the Client with responding to data subject requests and regulatory inquiries.
- Notify the Client without undue delay upon becoming aware of a data breach affecting personal data.

9.3 The Client warrants that it has a lawful basis for processing the personal data transmitted through the API and shall comply with all data protection obligations applicable to data controllers.

10 TERM & TERMINATION

10.1 This Agreement shall remain in effect until terminated by either party with 30 days' prior written notice.

10.2 amnis may suspend or revoke API access immediately:

- In the event of non-compliance with this Agreement.
- Due to a confirmed or suspected data breach.
- Following instructions from regulatory authorities.

10.3 Upon termination, the Client shall:

- Cease all API access and usage.
- Destroy or return all Confidential Information.
- Certify deletion of all API-derived data.

11 INTELLECTUAL PROPERTY

11.1 All rights, title, and interest in the API, documentation, and platform technologies remain the exclusive property of amnis.

11.2 The Client is granted no IP rights except as explicitly stated in this Agreement.

12 LIMITATION OF LIABILITY

12.1 Neither party shall be liable for indirect, incidental, or consequential damages, including lost profits, loss of data, or reputational harm.

12.2 amnis' total cumulative liability under this Agreement shall not exceed the total API fees paid by the Client in the 12 months preceding the event giving rise to the claim, unless caused by gross negligence, willful misconduct, or regulatory breach by amnis.

12.3 The Client assumes full liability for any breach resulting from its failure to implement minimum required API security controls, including but not limited to 2FA, credential rotation, and rate limiting.

13 INDEMNIFICATION

13.1 The Client agrees to indemnify and hold harmless amnis from and against all claims, damages, and losses arising out of:

- Breach of applicable laws or regulations.
- Unauthorized API access due to Client-side negligence.
- Claims by End Users relating to the Client's services or data handling.

13.2 amnis will provide reasonable cooperation and notice in the event of a third-party claim.

14 GOVERNING LAW & DISPUTE RESOLUTION

14.1 This Agreement shall be governed exclusively by the laws of Liechtenstein, without regard to conflict of law principles.

14.2 Any dispute arising from or relating to this Agreement shall be resolved by arbitration seated in Vaduz, Liechtenstein, in English, in accordance with the Liechtenstein Arbitration Association Rules. The arbitral decision shall be final and binding.

15 MISCELLANEOUS

15.1 This Agreement constitutes the entire agreement between the parties with respect to the API.

15.2 Amendments must be in writing and signed by authorized representatives.

15.3 The Client may not assign this Agreement without prior written consent from amnis.

15.4 If any provision is found unenforceable, the remainder of the Agreement shall remain in effect.

15.5 Sections regarding confidentiality, data handling, liability, and dispute resolution shall survive termination.