AMNIS EUROPE AG
Gewerbeweg 15
FL – 9490 Vaduz

# amnis

# AI Use Statement

## Introduction

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"), integrates artificial intelligence (AI) and machine learning (ML) into its operations in a transparent and responsible manner. These technologies are used to support — not replace — human decision-making, consistent with amnis' regulatory obligations and commitment to operational integrity. This statement explains how AI is applied within amnis services, outlines the principles and controls that govern its use, and reaffirms that all activities involving AI remain subject to human oversight, risk management, and applicable law.

## 1 Purpose and Scope

1.1. This statement articulates how amnis Europe AG, a licensed payment institution regulated by the Financial Market Authority (FMA) Liechtenstein, uses artificial intelligence (AI) and machine learning (ML) in its products and internal operations.

1.2. It applies to all services offered by amnis, including expense and card management, accounts payable and receivable, currency management, and related client-support functions. It also applies to AI features embedded in third-party tools that amnis engages as processors, including in product-analytics tooling used to improve the amnis webapp, and to enterprise AI assistants used by amnis personnel across departments to support internal operations (such as compliance, onboarding, legal, finance, marketing and operations).

1.3. The statement complements the framework agreement, privacy notice (GDPR / DSG), and product-specific terms and conditions.

1.4. amnis uses AI to enhance efficiency, accuracy, and client experience — never to autonomously execute payments or take decisions that could change a client's financial position without human approval.

## 2 How AI is Used Within amnis Services

2.1 AI capabilities are integrated in limited, controlled ways, for example:

- Client-support assistance — generating suggested responses, summarising knowledge-base content, and routing inquiries to human agents.
- Document & receipt inference — classifying uploaded receipts or invoices to assist in expense management.
- Transaction & anomaly flagging — detecting unusual activity patterns to support compliance and operations teams; all alerts are reviewed by authorised personnel before any action is taken.
- Automated summarisation & drafting — producing draft narratives or overviews in reports and dashboards for user review.
- Product-analytics AI assistance — within the product-analytics tooling used by amnis, pseudonymised behavioural data about how the webapp is used may be queried through AI-enabled features offered by the relevant provider. Such features may include natural-language interfaces that let authorised internal users query the pseudonymised data and integrations with external AI tools that allow authorised internal users to query the same data from approved internal clients. These features may rely

on generative-AI sub-processors engaged by the product-analytics provider; where the provider offers EU-instance routing for these features, amnis selects it. Features that are available within the subscription but not activated by amnis (for example more granular session-recording features or other advanced AI add-ons) are not used to process data.

- Cross-departmental AI assistant for internal operations — amnis uses one or more enterprise AI assistants (general-purpose AI tools provided by third-party AI service providers) across departments to support a range of internal tasks, including drafting and summarisation, document review, knowledge retrieval and analysis, research and structured data extraction. These assistants are also used in compliance and onboarding operations to support — but not replace — human reviewers during Know-Your-Customer and Know-Your-Business (KYC / KYB) onboarding evaluations, for example by extracting and structuring information from uploaded documents, by surfacing relevant context from internal sources, and by drafting initial assessments for human review. The safeguards that apply to this use are set out in Section 2.3.

2.2 Feature availability differs by product and service. AI operates as a support function within supervised processes and does not independently authorise, reject, or execute transactions.

2.3 Specific safeguards for AI-assisted KYC / KYB onboarding.

- Human-in-the-loop: final acceptance, rejection or escalation of an onboarding case is always made by an authorised member of amnis compliance staff. The AI assistant's output is treated as a draft for human review.
- No autonomous decisions about natural persons: AI assistants are not used to make automated individual decisions within the meaning of Article 22 GDPR. The outputs are reviewed and the decision is taken by amnis personnel.
- Data minimisation: only the documents and information necessary for the onboarding assessment are submitted to the AI assistant, in line with the principles of Article 5 GDPR.
- Confidentiality and access control: access to AI assistants inside amnis is restricted to authenticated employees through controlled enterprise channels; queries are logged in line with Section 4.
- No model training on client data: amnis has confirmed contractually with each of its AI service providers that prompts and outputs processed in the course of amnis' use of their service are not used to train the underlying AI providers' models (see Section 4.2).
- Risk and resilience: each AI service provider used by amnis is recorded in the amnis ICT third-party register and is subject to the controls described in Section 5.

# 3 Key Principles Guiding AI Use

## 3.1 Transparency

Clients and users are informed whenever they interact with AI-enabled functionality. amnis avoids and does not deploy deceptive or "dark-pattern" interfaces.

## 3.2 Human Oversight

Every process capable of affecting client funds, compliance, or regulatory reporting includes mandatory human review.

## 3.3 Accuracy and Limitations

AI-generated content may be incomplete or inaccurate. Outputs are provided "as is" and are not financial, legal, or regulatory advice. All material outcomes are validated by trained staff or authorised users before reliance.

## 4 Data Use, Logging, and Retention

4.1 AI systems process only the data required for their specific function and follow the principles of lawfulness, fairness, data minimisation, and storage limitation under Article 5 GDPR.

4.2 NO client data are used to train AI models unless expressly agreed in writing. This applies equally to (i) client data that may be processed through AI features embedded in third-party tooling engaged by amnis (including the product-analytics AI features described in Section 2.1), and (ii) client data that may be processed through the enterprise AI assistants used by amnis personnel for the cross-departmental purposes described in Section 2.1: amnis has contractually required that prompts and outputs processed through those features and assistants are not used to train the underlying AI providers' or the third-party tools' own models.

4.3 Logging — To maintain security and traceability (as required under Article 12 EU AI Act), amnis records limited technical information about AI inputs and outputs.

4.4 Retention — Logs are kept for at least 90 days, unless a longer period is required for legal, AML, or monitoring obligations. The retention period for the pseudonymised behavioural data processed by the product-analytics provider is set out in the amnis privacy notice.

4.5 Logged data are used only for internal diagnostics, service improvement, and regulatory compliance, are never sold or shared, and are protected by access controls consistent with GDPR and DORA security requirements.

## 5 Security and Operational Resilience

5.1 AI services and vendors form part of the ICT risk framework required under the Digital Operational Resilience Act (DORA). This includes both stand-alone AI service providers (including providers of general-purpose AI models within the meaning of Articles 51 to 55 of the EU AI Act) and AI features embedded in third-party tools engaged by amnis (including the product-analytics tooling referred to in Section 2.1 and its generative-AI sub-processors). The current list of AI service providers used by amnis is maintained in the internal AI system register described in Section 6.2.

5.2 amnis:

- maintains an ICT third-party register covering AI providers;
- performs risk-based due diligence and contractual oversight;
- monitors system performance and continuity;
- applies incident-classification and reporting procedures consistent with PSD2 and DORA obligations.

5.3 Any material incident involving AI that could affect service quality or client operations is handled under the established incident-response framework and, where required, reported to the FMA.

## 6 Governance and Regulatory Alignment

6.1 AI activities fall under the same enterprise risk and compliance governance that covers ICT and operational risks.

6.2 amnis maintains an internal AI system register documenting each system's purpose, data use, providers and sub-processors, and oversight arrangements. The product-analytics AI features described in Section 2.1 and the cross-departmental enterprise AI assistants described in Section 2.1 are each recorded in this register, together with the data categories processed.. The register is the canonical source for the identity of the AI providers used by amnis and is updated when providers are added, changed or replaced.

6.3 Regular reviews ensure continued compliance with:

- PSD2 (Directive (EU) 2015/2366) — payment execution and liability rules;
- DORA (Regulation (EU) 2022/2554) — ICT risk and third-party management;
- GDPR / DSG — data-protection obligations; and
- EU AI Act (Regulation (EU) 2024/1689) — transparency, record-keeping, and human-oversight duties for deployers.

6.4 amnis currently operates no AI systems classed as "high-risk" under Annex III of the EU AI Act but will review new use cases periodically and implement conformity-assessment measures if that status changes. The product-analytics AI features described in Section 2.1 are assessed as not high-risk under Annex III. The cross-departmental use of enterprise AI assistants described in Section 2.1, including their supporting role in KYC / KYB onboarding, is also assessed as not high-risk under Annex III on the basis that the AI assistants are used as support tools for human reviewers, no automated individual decisions about natural persons are taken (Section 2.3, Article 22 GDPR), and decisions remain with qualified amnis personnel. amnis will treat any change to this configuration — including any move towards autonomous decisioning, automated risk scoring of natural persons or other functionality engaging Annex III, point 5(b) or point 6 — as a trigger for re-classification, a fresh conformity assessment, and (where applicable) the introduction of the additional controls required of deployers of high-risk AI systems. Where amnis relies on a provider of a general-purpose AI model within the meaning of Articles 51 to 55 of the EU AI Act, the provider is monitored against the GPAI provider obligations through the ICT third-party register described in Section 5.

## 7 Client Assurances

7.1 AI does not autonomously execute or authorise payments.

7.2 All client instructions remain subject to explicit user confirmation and existing authentication controls (e.g., SCA under PSD2).

7.3 amnis remains fully responsible for compliance with applicable payment-service obligations, irrespective of the use of AI tools.

## 8 Continuous Improvement and Review

8.1 AI deployment is an evolving area. amnis reviews this statement and its underlying controls at least annually, or sooner if regulatory guidance changes. Updates are communicated through the usual client-communication channels and reflected in the applicable terms & conditions.

Edition: June 2026