

**amnis**

# **AI Use Statement**

- INTRODUCTION ..... 3**
- 1 PURPOSE AND SCOPE ..... 4**
- 2 HOW AI IS USED WITHIN AMNIS SERVICES ..... 4**
- 3 KEY PRINCIPLES GUIDING AI USE..... 5**
- 4 DATA USE, LOGGING, AND RETENTION ..... 5**
- 5 SECURITY AND OPERATIONAL RESILIENCE ..... 6**
- 6 GOVERNANCE AND REGULATORY ALIGNMENT..... 6**
- 7 CLIENT ASSURANCES ..... 7**
- 8 CONTINUOUS IMPROVEMENT AND REVIEW ..... 7**

## 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.
- 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.
- 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.

### 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.
- 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.
- 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).

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, and oversight.

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.

## **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.