AML / KYC Statement

Cemperium is committed to operating a transparent, compliant, and responsible platform. This statement outlines how Anti-Money Laundering (AML) and Know Your Customer (KYC) obligations are addressed within the Cemperium ecosystem — and what that means for users, partners, and regulators.

Contact Compliance Team

Review Privacy Policies

SECTION 1

Introduction

This statement outlines how Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements are handled in connection with the Cemperium platform. It is intended to provide clarity to platform users, integration partners, and regulatory stakeholders regarding the distribution of compliance responsibilities across the ecosystem.

AML and KYC frameworks exist to protect the integrity of financial systems worldwide. They are designed to prevent the facilitation of illegal activities — including money laundering, terrorist financing, and fraud — by ensuring that the identity of individuals accessing financial services is properly verified and that transactions are appropriately monitored.

Cemperium is committed to supporting full compliance with all applicable regulations. This commitment manifests not through direct regulatory action, but through a deliberate and structured approach: partnering with authorized, regulated entities who carry out the required procedures on behalf of end users. This statement documents that approach with transparency and precision.

Why This Statement Matters

Transparency

Clear disclosure of how compliance is managed across the platform.

Accountability

Defined roles for Cemperium, partners, and users.

Regulatory Clarity

Alignment with applicable AML/KYC regulatory frameworks.

SECTION 2

Platform Role

Cemperium operates exclusively as a technology platform. It provides the infrastructure, user interfaces, and integration capabilities that enable financial services to be delivered — but it does not itself perform KYC or AML procedures, nor does it act as a regulated financial institution in any jurisdiction.

This distinction is both deliberate and structurally important. Regulated financial activities — including identity verification, customer due diligence, and transaction monitoring — require specific authorizations and are governed by strict legal frameworks that apply to entities directly performing those activities. Cemperium's role is to provide the technological foundation upon which such regulated activities can take place through appropriately licensed partners.

Technology Provider

Cemperium supplies the infrastructure and interfaces that power platform functionality.

Not a Financial Institution

Cemperium does not hold regulatory licenses to perform financial services directly.

Compliance Enabler

The platform is architected to enable regulated partners to fulfill their obligations seamlessly.

SECTION 3

Partner-Based Compliance

AML and KYC procedures on the Cemperium platform are conducted by regulated third-party partners who are fully integrated into the platform's service delivery architecture. These partners hold the regulatory authorizations necessary to perform compliance functions legally and are independently accountable for fulfilling their obligations under applicable law.

By routing compliance procedures through authorized partners, Cemperium ensures that users are served by entities equipped and licensed to handle sensitive financial compliance tasks. Each partner operates under its own regulatory framework, which may vary by jurisdiction, service type, and applicable law. This structure allows the platform to serve a diverse range of use cases while maintaining robust compliance integrity throughout.

User Identity Verification

Partners are responsible for verifying the identity of users accessing regulated services, in accordance with applicable KYC standards.

Customer Due Diligence

Partners conduct thorough CDD processes to assess user risk profiles and ensure suitability for the services being accessed.

Transaction Monitoring

Ongoing monitoring of transactions is carried out by partners to detect suspicious activity and flag potential compliance issues.

Regulatory Reporting

Partners are responsible for submitting required reports to relevant financial intelligence units and regulatory bodies.

SECTION 4

When KYC Is Required

Not all interactions with the Cemperium platform require identity verification. KYC procedures are triggered only when users seek to access specific services that fall within the scope of regulated financial activity. This approach reflects a proportionate compliance posture — applying verification where it is legally required, and avoiding unnecessary friction where it is not.

When KYC is required, users will be directed clearly and seamlessly to the relevant regulated partner for verification. The process is managed by that partner and governed by its own policies and regulatory obligations. Users should expect to provide documentation and information consistent with standard financial KYC requirements.

Failure or refusal to complete required verification will result in restricted access to the services for which verification is required. This is not a discretionary measure — it reflects a mandatory compliance requirement that Cemperium and its partners are obligated to enforce.

Services That Trigger KYC

Fiat Onboarding

Accessing services that involve traditional currency requires verified identity.

Payment Processing

Initiating or receiving payments through regulated payment channels triggers KYC requirements.

On-Ramp & Off-Ramp Services

Converting between fiat and digital assets requires partner-conducted identity verification.

Users will be guided to the relevant partner for verification when accessing any of the above services. Completion of verification is mandatory.

SECTION 5

Data Handling

Personal data collected during KYC processes — including identity documents, biometric data, and financial information — is handled exclusively by the third-party provider conducting the verification. Cemperium does not store, process, or control sensitive verification data unless it is explicitly and necessarily required for core platform functionality.

This separation is intentional. By limiting Cemperium's access to sensitive compliance data, the platform minimizes data exposure and reduces the risk of unauthorized access or misuse. Each third-party provider is responsible for implementing appropriate data security measures, retaining data in accordance with applicable retention requirements, and ensuring compliance with relevant data protection laws — including, where applicable, the GDPR and equivalent regional frameworks.

Users are strongly encouraged to review the privacy policies of the specific providers they interact with during the verification process. These policies govern how personal data is collected, stored, used, and shared. Questions regarding data held by a specific provider should be directed to that provider directly. For broader platform-level data inquiries, users may contact Cemperium at **legal@cemperium.se**.

Data Controller

The third-party KYC partner — not Cemperium — acts as the data controller for verification data.

Minimal Data Access

Cemperium only accesses data that is strictly necessary for platform functionality.

User Rights

Users should refer to the relevant provider's privacy policy to understand their rights and how data is used.

SECTION 6

Compliance Objectives

The structural approach Cemperium has adopted — routing regulated compliance functions through authorized third-party partners — is not merely an administrative arrangement. It reflects a deliberate set of compliance objectives that are central to the platform's design and operating philosophy.

Ensure AML Regulatory Compliance

The platform structure is designed to ensure that all regulated activities carried out within or through the platform are subject to appropriate AML controls. By partnering with authorized entities, Cemperium ensures that the AML compliance framework is implemented by those legally equipped and obligated to do so.

Prevent Misuse of Financial Systems

A core objective of the platform's compliance architecture is to prevent Cemperium's infrastructure from being used as a vehicle for money laundering, terrorist financing, fraud, or any other form of financial crime. The KYC and monitoring procedures performed by partners serve as essential safeguards against such misuse.

Maintain Clear Separation of Responsibilities

Clarity of roles is fundamental to sound compliance governance. Cemperium's framework clearly delineates what the platform does, what regulated partners do, and what is expected of users. This separation reduces ambiguity, minimizes compliance risk, and supports accountability at every level of the ecosystem.

SECTION 7

User Responsibility

Compliance is a shared responsibility. While Cemperium and its regulated partners maintain the structural and procedural frameworks required by law, users play an essential and non-delegable role in ensuring that compliance obligations are met at the individual level.

Users are required to engage honestly and cooperatively with verification processes. Providing false, misleading, or incomplete information during KYC procedures is not only a violation of platform terms but may also constitute a criminal offense under applicable law. All users are expected to understand the legal context in which they are operating and to take their compliance obligations seriously.

It is also the user's responsibility to be aware of when third-party verification is required. Cemperium will provide clear guidance and direction at the point of service access, but users should not assume that a lack of prompt necessarily means verification is not required. When in doubt, users are encouraged to seek clarification before proceeding.

What Users Must Do

1 Provide Accurate Information

Submit truthful, complete, and up-to-date information during all verification processes.

2 Comply with Applicable Laws

Understand and adhere to the legal requirements that apply to your jurisdiction and use case.

3 Complete Required Verification

Recognize when third-party KYC is required and complete it promptly to avoid service restrictions.

⚠ Failure to complete required verification may result in restricted or suspended access to certain platform services.

SECTION 8

Monitoring and Restrictions

Access to certain features and services on the Cemperium platform may be restricted based on a combination of regulatory requirements, partner-specific policies, and jurisdictional limitations. These restrictions are not arbitrary — they reflect binding legal obligations and risk management determinations made in accordance with applicable compliance frameworks.

Regulatory requirements may prohibit or condition the provision of specific services to users in particular jurisdictions, or to users who have not completed required verification procedures. Partner policies may impose additional eligibility criteria based on the risk profile of the user or the nature of the requested service. Jurisdictional limitations reflect the reality that financial regulations vary significantly across borders, and that services lawfully available in one country may be restricted or prohibited in another.

Cemperium reserves the right to restrict, suspend, or terminate access to any feature or service where such action is required for compliance purposes. This right is exercised responsibly and proportionately, but it is not subject to negotiation where a binding compliance obligation exists. Users who believe a restriction has been applied in error are encouraged to contact the compliance team for clarification.

1

Regulatory Requirements

Mandatory legal obligations may restrict access for certain users or service categories.

2

Partner Policies

Regulated partners may apply eligibility criteria that further limit service availability.

3

Jurisdictional Limitations

Services may be unavailable in jurisdictions where regulatory restrictions apply.

SECTION 9 & 10

Updates & Contact

Statement Updates

This AML/KYC Statement may be updated periodically to reflect changes in applicable regulatory requirements, platform structure, partner arrangements, or operational practices. Regulatory environments evolve — and Cemperium is committed to ensuring that this statement remains accurate, current, and reflective of actual platform operations at all times.

Users are strongly encouraged to review this page on a regular basis. Significant changes will be communicated through appropriate platform channels where practicable, but the responsibility for staying informed ultimately rests with the user. Continued use of the platform following an update to this statement constitutes acceptance of the revised terms.

Where a regulatory change materially affects user obligations or access to services, Cemperium will make reasonable efforts to provide advance notice. However, where immediate compliance action is required by law, updates may take effect without prior notice.

Get in Touch

For all inquiries related to AML/KYC compliance, including questions about verification requirements, partner procedures, jurisdictional restrictions, or data handling practices, please contact the Cemperium compliance team directly.

📧 **Compliance & Legal Inquiries:**
legal@cemperium.se

Our compliance team will respond to all inquiries in a timely and professional manner. For urgent matters, please indicate the nature and urgency of your inquiry in the subject line of your email.

Email legal@cemperium.se