AI Legal and Banking Checklist

An AI product should be legally structured before it enters the market. For banks, PSPs, investors and B2B clients, it is important to see not only the technology itself, but also the company's overall legal readiness: who owns the product, which entity provides the service, which contracts govern relationships with users and contractors, who holds the IP rights, how data is processed, and which compliance risks have already been addressed. These elements form the foundation of an AI company's legal and banking readiness.

Regulatory Landscape:

Core AI and Data Regulation

AI businesses operating in or targeting the EU should first assess whether their products fall within the scope of the **EU AI Act** and the **GDPR**.

The AI Act may apply depending on the role of the company (for example, provider or deployer), the intended use of the system and the risk category of the AI solution. The GDPR becomes relevant where the product processes personal data, including user inputs, account data, behavioural data or data used in model training, analytics or profiling.

Commercial, Contractual and IP Framework

AI companies also need a clear legal basis for the way their product is offered and monetised. This usually includes Terms of Use, B2B agreements, API terms, data processing documentation and a clear contractual allocation of rights and responsibilities.

From an IP perspective, the company should be able to demonstrate rights to the code, product architecture, datasets, prompts, documentation, branding and other key business assets, as well as a compliant use of third-party models, open-source components and external technology providers.

Banking, Payments and Financial Perimeter

Where an AI company needs merchant acquiring, PSP onboarding, cross-border payments, recurring billing or crypto-related functionality, banking and payments regulation becomes commercially relevant. Depending on the business model, the company may need to consider the **Payment Services Directive (PSD2)**, the **E-Money Directive**, AML / sanctions expectations and, where relevant, the **MiCA Regulation**.

Even where these rules do not directly apply, banks and PSPs will still expect a transparent business model, clean documentation and clearly explainable payment flows.

Sector-Specific Regulation

Additional legal review is often needed where AI is used in regulated or sensitive sectors such as financial services, health, employment, education, legal services or access to essential services. In these cases, the AI product may trigger both AI-specific rules and sector-specific compliance obligations.

What May Fall Under Regulation?

An AI business is more likely to require enhanced legal review where it:

- processes personal data or behavioural data;
- uses AI in recruitment, lending, insurance, healthcare, education or legal services;
- generates outputs that may affect users' rights or economic interests;

- relies on third-party models, datasets or open-source components;
- offers subscriptions, recurring billing, cross-border payments or marketplace flows;
- integrates wallets, stored balances, payouts or crypto-related features;
- operates across multiple jurisdictions or targets EU customers.

Company Structure

☐ The company legally providing the AI service to clients and responsible for the product has been clearly identified.

☐ The chosen jurisdiction is aligned with the business model, target markets, tax considerations, banking expectations and investor requirements.

☐ The ownership structure, as well as the roles of founders, directors, shareholders and key project participants, are clear and properly documented.

☐ If the business uses a holding company, operating company or separate IP company, the function of each entity is clearly defined and separated.

Contracts

☐ Terms of Use / Terms of Service have been prepared and reflect how the AI product actually operates.

☐ For a B2B model, a SaaS Agreement, Service Agreement or API Terms have been prepared depending on how the product is provided to clients.

☐ The Privacy Policy, Data Processing Agreement and AI Disclaimer are aligned with the actual data flows, AI functionality and the company's role in relation to users.

☐ Agreements with developers, employees, consultants and contractors include IP assignment, confidentiality and restrictions on the use of confidential business information.

☐ Client-facing contracts include provisions on limitation of liability, acceptable use of the AI service, prohibited use cases and the status of AI-generated outputs.

Intellectual Property

☐ The company's rights to the code, product architecture, design, technical documentation and other key IP assets have been confirmed.

☐ The legal status of AI models, datasets, prompts, user inputs and AI-generated outputs used in the product has been reviewed.

☐ The terms of use of third-party AI tools, open-source components, data providers and other external technology solutions have been analysed.

☐ The product terms define who owns user inputs and AI outputs, and how they may be used by the company and by users.

Compliance

☐ The company has identified which personal data is collected, processed, stored, transferred to third parties or used within the AI functionality.

☐ The applicability of the GDPR and the need for a Privacy Policy, Data Processing Agreement, DPIA or other data protection documents have been assessed.

☐ A preliminary assessment of the AI Act risk category has been conducted, taking into account the product's functions, target users and intended use.

☐ It has been assessed whether the product is used in high-risk or regulated sectors and therefore requires additional legal review.

☐ Users are provided with clear information on the use of AI, the limitations of AI-generated outputs and the limits of the company's liability.

2. AI Banking Guide

An AI company's banking readiness depends on how clearly it can explain its business model, customer base, sources of revenue, payment flows and product risk profile. For banks and PSPs, it is important to see a transparent operational structure, clear documentation and basic controls addressing AML exposure, fraud, chargebacks and regulatory risks.

Bank Requirements

☐ A concise description of the AI product, business model, target markets, customers and revenue sources has been prepared.

☐ It has been determined whether the product operates in regulated or sensitive sectors, such as finance, health, employment, education, legal services or crypto.

☐ A basic onboarding package has been prepared, including corporate documents, ownership structure, UBO information, management details and website / product description.

☐ The pricing model, source of funds, source of revenue and expected transaction volumes can be clearly explained to a bank or PSP.

PSP Onboarding

☐ The appropriate payment setup has been selected, such as card acquiring, subscriptions, payouts, marketplace payments or cross-border payments.

☐ The customer journey, payment flow, refund rules, chargeback management and fraud prevention controls have been documented.

☐ The Terms of Use, Privacy Policy, pricing page, refund policy and customer support process are aligned with PSP requirements.

☐ It has been checked whether the PSP accepts the relevant AI use case, target markets, payment methods and risk profile.

Payment Flows

☐ The flow of funds has been described: who pays, what they pay for, who receives the funds, when the funds are charged, and how refunds or payouts are made.

☐ It has been determined whether the company accepts payments only for its own services or also participates in the transfer of funds between third parties.

☐ The subscription, usage-based billing, API billing or commission model is reflected in the contracts, pricing terms and payment infrastructure.

☐ Crypto payments, where used, have been separately assessed from the perspective of AML, banking acceptance, tax, refunds and volatility risks.

3. AI Compliance Roadmap

AI compliance should not be built around formal documents alone, but around the actual use case: what function the AI system performs, what data it processes, who may be affected by its outputs, and what risks may arise for users, clients and the business. For an AI company, a basic compliance roadmap should combine the requirements of the EU AI Act, the GDPR and an internal risk assessment.

EU AI Act

☐ The company's role in relation to the AI system has been identified: provider, deployer, importer, distributor or product manufacturer.

☐ A preliminary classification of the AI system has been conducted: prohibited AI practice, high-risk AI system, AI system subject to transparency obligations or lower-risk AI.

☐ It has been checked whether the AI product is used in areas that may create increased regulatory risk, such as employment, education, finance, health, law enforcement or access to essential services.

☐ Basic AI disclosures have been prepared for users where they interact with an AI system or receive AI-generated outputs.

GDPR

☐ Data mapping has been conducted: what personal data is collected, from which sources, for what purposes, where it is stored and to whom it is disclosed.

☐ The legal basis for each key processing activity has been identified, including training, analytics, profiling or automated decision-making.

☐ The Privacy Policy, Data Processing Agreement, cookie / tracking disclosures and vendor data protection clauses have been prepared or updated.

☐ The need for a DPIA has been assessed, especially where the AI system processes sensitive data, conducts profiling or may significantly affect users.

Risk Assessment

☐ The key risks of the AI product have been described, including data protection, bias, hallucination, misuse, cybersecurity, consumer protection, contractual liability and sector-specific risks.

☐ Risk controls have been identified, such as human oversight, user warnings, access restrictions, logging, monitoring, content moderation or an escalation process.

☐ The limitations of the AI system, permitted use cases, prohibited use scenarios and user responsibilities have been documented.

☐ A process has been established for periodic review of AI risks after launch, model updates, changes in data flows or expansion into new markets.

4. AI Payment Infrastructure Guide

An AI company's payment infrastructure should reflect not only user convenience, but also the legal nature of the business model. It is important to determine whether the company simply accepts payments for its own AI service, or whether it is involved in holding, distributing, transferring or converting funds. This directly affects the choice of PSP, the need for an EMI partner and the acceptability of crypto payments.

PSP

☐ The required payment methods have been identified, such as card payments, subscriptions, recurring billing, invoices, payouts or cross-border payments.

☐ The selected PSP is aligned with the business model, target markets, currencies, transaction volumes and risk profile of the AI product.

☐ The payment page, pricing terms, refund policy, customer support process and Terms of Use are aligned with PSP requirements.

☐ It has been checked whether the PSP accepts the relevant AI use case, including regulated or sensitive sectors.

EMI

☐ It has been assessed whether the business model requires an EMI / payment institution partner, especially where wallets, stored balances, payouts or movement of funds between users are involved.

☐ It has been determined whether the company accepts payments only for its own services or effectively participates in payment services for third parties.

☐ It has been checked whether there is any risk of unauthorised payment services, e-money issuance or custody of client funds.

☐ The roles of the AI company, PSP, EMI and other payment partners are clearly reflected in contracts and user-facing documents.

Crypto Payments

☐ It has been determined whether crypto payments are used as a payment method for the company's own service or as part of a broader financial or payment model.

☐ AML, sanctions, Travel Rule, tax, accounting, refund and volatility risks related to accepting crypto payments have been assessed.

☐ It has been checked whether the use of crypto payments may negatively affect the company's banking / PSP onboarding or risk classification.

☐ The Terms of Use and payment terms describe the process for accepting crypto payments, refunds, conversion, transaction finality and user responsibility.

5. AI Business Model Framework

The legal assessment of an AI company always starts with its business model. Banks, investors, clients and regulators need to understand how the product is provided to users: as a SaaS platform, an API solution, an embedded AI module or a customised service. This determines the applicable contracts, liability structure, data flows, pricing model, IP rights and compliance requirements.

SaaS

☐ It has been determined whether the AI product is provided as a self-service platform, B2B SaaS, enterprise solution or white-label product.

☐ The customer journey has been described, including registration, access to features, use of the AI system, payment, support and termination of access.

☐ The SaaS Agreement / Terms of Use define the scope of service, acceptable use, restrictions, service availability, support, suspension and termination rules.

☐ The pricing model — subscription, usage-based billing, freemium or enterprise fee — is aligned with the contracts, payment infrastructure and billing process.

☐ It has been determined what data users upload to the system, whether such data is used for training / improvement, and how this is reflected in the Privacy Policy and contractual terms.

API

☐ It has been determined whether the API is used to provide access to AI functionality, integrate with client products or enable automated data processing.

☐ The API Terms define access rules, authentication, rate limits, permitted use, prohibited use, monitoring, suspension and liability allocation.

☐ The data transferred through the API has been described, including who acts as controller / processor and which data protection obligations apply.

☐ The parties' responsibility for integration errors, misuse, security incidents, inaccurate outputs or downstream use of AI-generated results has been defined.

☐ API pricing, usage limits, billing metrics and technical documentation are aligned with commercial terms and payment infrastructure.