IntelliSecure

INSIGHTS

FRANCE TO REQUIRE LICENSING FOR DIGITAL ASSET SERVICE PROVIDERS IN JANUARY 2024 - UPDATE



France to Require Licensing for Digital Asset Service Providers in January 2024

On 20 April 2023, the European Parliament passed the Markets in Crypto Assets (MiCA) regulation. However, one of its member states (France) has been getting a head start in tightening the regulation of digital assets since the first quarter of this year.

Currently, digital asset service providers (DASPs) must register with the French financial authorities (*Autorité des marchés financiers* or AMF) if they wish to provide any of the following services in France:

- digital asset custody
- buying or selling digital assets in a currency that is legal tender
- trading of digital assets against other digital assets
- operation of a trading platform for digital assets.[1]

Licensing is optional, and the AMF has not licensed any DASP to date. However, that is all set to change.

On 9 February 2023, France's Parliament introduced legislation requiring DASPs to obtain licenses from January 2024. Approved on 28 February 2023, it now awaits the president's approval to be signed into law.

Insight 1: Registration Is No Longer an Option for New DASPs

With 10 months until licensing becomes mandatory, the timeline to submit DASP registration applications to the AMF is exceptionally tight. Therefore, DASPs that wish to commence operations in France from 2024 onwards should prepare license applications instead of registration applications.

Footnotes

[1] *See* https://www.amf-france.org/en/professionals/fintech/my-relations-amf/obtain-dasp-authorisation#Focus_on_digital_asset_services.

Insight 2: Registered DASPs Should Be Preparing for MiCA Compliance

Whether existing registered DASPs will be required to convert to licenses from January 2024 remains unclear (there are currently over 60 registered with the AMF). This makes the timeline to ensure compliance with licensing requirements exceptionally tight.

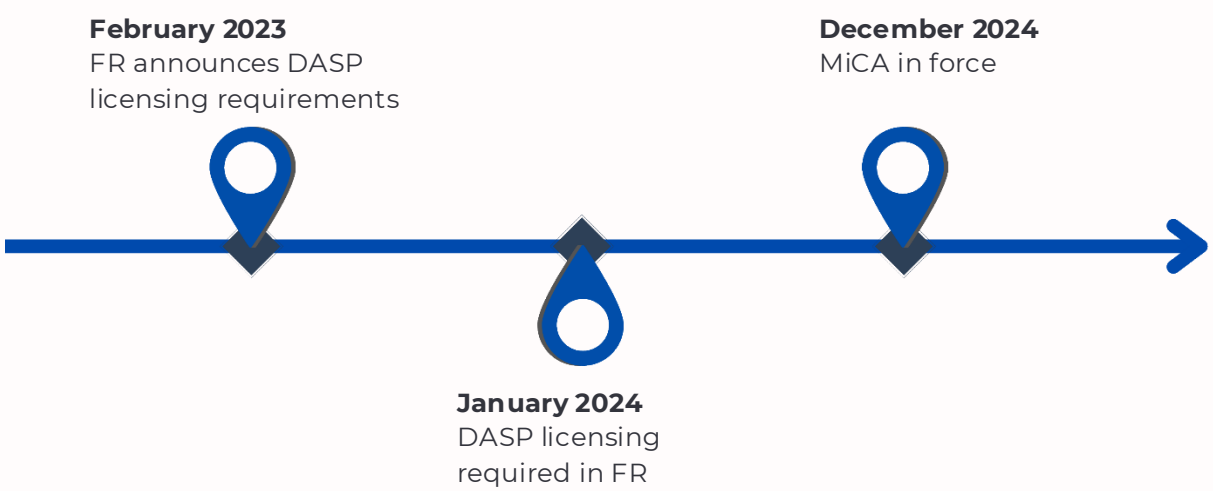
DASP licensing requirements are markedly more onerous than registration requirements. Registration focuses on governance and AML/CFT (anti-money laundering/combatting terrorism financing) processes. Licensing includes requirements regarding financial viability, staffing, internal controls, IT systems, and client safeguards.

While the starting point for French DASPs is to comply with French regulatory requirements, compliance does not have to stay that way. As MiCA expands its potential market share to the European Union, ensuring MiCA compliance should be considered a strategy for expanding into Europe and beyond.

The legislation has been implemented in phases :

- Title XI and XII (Stablecoins): These parts of MiCA became effective on June 30, 2024.
- Other parts of MiCA: Most of the remaining provisions will apply from December 30, 2024.

Timeline of French DASP regulatory compliance



Insight 3: Position Compliance as Good Business Practice (Versus Merely Adhering to Regulatory Requirements)

Given the fallout of the current crypto winter, customers have grown increasingly skeptical of the sustainability of DASPs – will their service providers be here today and gone tomorrow? Can DASPs be trusted with one's digital assets?

DASPs that signal their intention and plans for regulatory compliance as a good business practice provide a reassuring indicator that they are in it for the long run.

DASPs that signal their intention and plans for regulatory compliance as a good business practice provide a reassuring indicator that they are in it for the long run.

Insight 4: Examples of How DASPs Can Comply with Regulations (cont)

Below are some examples of how DASPs can comply with regulations, bearing in mind that the specifics will depend on the precise services they provide and the relevant regulations (MiCA and French national rules):

Authorisation/Licensing Requirements:

- DASPs must obtain the necessary authorisation or license from the relevant authorities (e.g., AMF in France) before providing regulated services.
- This involves meeting specific requirements related to capital, governance, internal controls, and operational resilience.

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF):

- Implement robust AML/CTF policies and procedures.
- Conduct thorough Know Your Customer (KYC) checks on clients.
- Monitor transactions for suspicious activity and report it to the authorities.
- Comply with record-keeping requirements.

Custody Requirements:

- If custody services are provided, DASPs must ensure the safe and secure storage of clients' digital assets.
- This may involve segregating client assets from the DASP's assets, implementing strong cybersecurity measures, and implementing contingency plans.

Conduct of Business Rules:

- DASPs must act honestly, fairly, and professionally in the best interests of their clients.
- This includes providing clear and accurate information to clients, avoiding conflicts of interest, and ensuring fair treatment.

Insight 4: Examples of How DASPs Can Comply with Regulations

Prudential Requirements:

- MiCA introduces prudential requirements for issuers of stablecoins and for DASPs providing certain services.
- These requirements ensure these entities have sufficient capital to withstand risks and protect consumers.

Governance and Internal Controls:

- DASPs must have robust governance arrangements, including a clear organisational structure, well-defined responsibilities, and effective oversight mechanisms.
- They must also implement sufficient internal controls to manage risks, ensure compliance, and protect client assets.

Cybersecurity:

- Given the nature of digital assets, cybersecurity is paramount.
- DASPs must implement robust cybersecurity measures to protect their systems and client assets from cyber threats. These measures include risk assessments, security policies, incident response plans, and regular security testing.

Important Note:

- Regulatory requirements are complex and can vary depending on the specific activities of a DASP.
- DASPs must stay up-to-date with regulatory developments and seek professional advice to ensure compliance.

For more information on these developments or their implications for your business, please contact contact@intellisecure.co

