

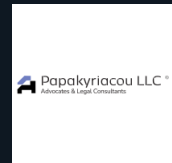
Legal 500

Country Comparative Guides 2025

Cyprus
Fintech

Contributor

Akis Papakyriacou LLC



Akis Papakyriacou

Managing Partner | akis@papakyriacoulaw.com

This country-specific Q&A provides an overview of fintech laws and regulations applicable in Cyprus.

For a full list of jurisdictional Q&As visit legal500.com/guides

Cyprus: Fintech

1. What are the regulators for fintech companies in your jurisdiction?

Fintech companies in the Republic of Cyprus, are regulated by the Central Bank of Cyprus (the "CBC") and/or the Cyprus Securities and Exchange Commission (the "CySEC"), depending on their activities, services and products.

2. Do you foresee any imminent risks to the growth of the fintech market in your jurisdiction?

We do not identify and/or anticipate any imminent risks to the growth of fintech, especially having in mind that CySEC has taken positive steps towards embracing fintech, therefore further positive developments are expected. The only potential hurdle in the development of fintech in Cyprus, especially in matters relating to cryptocurrencies, is the CBC's reluctant approach towards fintech and cryptocurrencies.

The European Union's newly implemented and forthcoming regulations, such as the Markets in Crypto Assets Regulation ("MiCA"), the AI Act under Regulation No. 2024/1689 (the "AI Act"), and the Digital Operational Resilience Act ("DORA"), are poised to significantly enhance Cyprus's fintech landscape. These initiatives aim to mitigate operational risks while bolstering the protection of financial services consumers, creating a safer and more robust environment for innovation and growth.

3. Are fintechs required to be licensed or registered to operate in your jurisdiction?

Yes, fintech companies are generally required to be licensed or registered to operate in the Republic of Cyprus, depending on the specific nature of their activities. The Republic of Cyprus follows EU regulations and directives, which means compliance requirements are aligned with European standards. Below are some key points regarding licensing and registration for fintech companies in the Republic of Cyprus:

For instance, fintech companies offering financial services such as payment processing or issuing electronic money must obtain a license from the CBC

pursuant to the Electronic Money Law 81(I)/2012 and to the Payment Services Law and the Provision and Use of Payment Services and Access to Payment Systems Laws 31(I)/2018.

Crypto-related businesses, including cryptocurrency exchanges or wallet providers, must be licensed by CySEC pursuant to MiCA.

Fintech companies involved in investment services, such as trading platforms, would likely need authorization under the Investment Services and Activities and Regulated Markets Law 87(I)/2017 (the "Investment Services Law"), while crowdfunding platforms facilitating investment or lending activities may need to adhere to the Provision of Crowdfunding Services for Businesses Law 123(I)/2024.

For startups testing innovative models that don't clearly fit into existing regulatory categories, Cyprus also provides opportunities to collaborate with the Central Bank of Cyprus Innovation Hub for guidance on potential licensing and compliance.

As regulations evolve, especially with new frameworks like MiCA and DORA, it's important for fintechs to regularly assess whether their activities require registration or licensing. The overall goal of these requirements is to ensure transparency, protect consumers, and support the growth of the fintech sector in Cyprus.

4. What is a Regulatory Sandbox and how does it benefit fintech start-ups in your jurisdiction?

A Regulatory Sandbox is a controlled environment set up by regulatory authorities that allows fintech start-ups and other innovative companies to test their products, services, or business models under real-world conditions, but with regulatory oversight.

On the 11th of June 2024, CySEC launched its Regulatory Sandbox, aiming to offer a platform for the testing of new technologies in a controlled environment. By allowing pioneering products, services, and business models to be trialed within a controlled and time-limited environment, the sandbox helps CySEC deepen its understanding of emerging technologies and supports ongoing regulatory adjustments to keep pace with evolving market trends.

The CBC has also launched an Innovation Hub, aiming to support and encourage organisations to address regulatory and administrative hurdles when promoting innovative technologies by providing non-binding guidance on regulatory and supervisory prerequisites including any potential licensing requirements for innovative fintech products or services. The CBC's innovation hub aims to support both start-ups and established companies looking to adopt innovative business models, integrate new technologies, or introduce groundbreaking services or products to the Cyprus market and beyond.

5. How do existing securities laws apply to initial coin offerings (ICOs) and other crypto assets, and what steps can companies take to ensure compliance in your jurisdiction?

ICOs, are potentially regulated by either MiCA or by the Investments Services Law (through which MiFID II was transposed to Cyprus law). MiCA explicitly excludes crypto-assets that qualify as financial instruments under Article 2. Therefore, where the asset subject to an ICO is classified as a financial instrument, the provisions of the Investment Services Law would apply. The distinction between these two regulatory frameworks is largely conceptual, and the classification of each asset should be evaluated on a case-by-case basis. It is important to note that the European Securities and Markets Authority (ESMA) has provided guidelines for the classification of crypto-assets as financial instruments. Consequently, issuers should seek expert legal advice and conduct a thorough assessment of the crypto-asset in question to ensure that the appropriate regulatory framework is applied.

MiCA, in its approach, adopts a pragmatic stance that appears advantageous for issuers. Specifically, under Article 4 of MiCA, which governs public offers of crypto-assets (excluding asset-referenced and e-money tokens), a notification to the regulator is required, rather than full authorization. This streamlined process could potentially reduce the regulatory burden for issuers.

6. What are the key anti-money laundering (AML) and Know Your Customer (KYC) requirements for cryptocurrency exchanges in your jurisdiction, and how can companies implement effective compliance programs to meet these obligations?

In Cyprus, Crypto Asset Service Providers (CASPs) are obligated to adhere to the provisions of the Prevention

and Suppression of Money Laundering and Terrorist Financing Law 188(I)/2007 (the "AML Law"). Under this legislation, CASPs must implement customer verification procedures and conduct due diligence when establishing a business relationship and/or when executing a transaction of €1,000 or more, whether this amount is reached through a single transaction or multiple potentially linked transactions.

It is also noted that the implementation of MiCA, as well as the imminent implementation of DAC 8, which takes effect on 1 January 2026, will play a key role on the AML and KYC requirements for cryptocurrency exchanges and related businesses.

7. How do government regulations requiring licensing or regulatory oversight impact the operations of cryptocurrency and blockchain companies in your jurisdiction, and what strategies can be employed to navigate these varying requirements?

Cyprus adheres to EU regulations and directives, therefore cryptocurrency and blockchain companies would need to comply with the requirements of the newly implemented MiCA in order to be licensed in Cyprus. It is important for companies looking to engage into regulated activities in and/or from Cyprus to seek professional advice in order to properly understand their obligations.

8. What measures should cryptocurrency companies take to comply with the governmental guidelines on tax reporting and obligations related to digital assets in your jurisdiction?

The imminent implementation of DAC8 in January 2026 expands the scope of the automatic exchange of information to include crypto-assets and e-money transactions. Under this framework, reporting crypto-asset service providers will be required to disclose information on transactions and transfers involving these assets. The proposed legislation aligns closely with MiCA, adopting similar definitions for crypto-asset service providers, crypto-asset services, and crypto-assets. In practice, reporting service providers will either be entities registered under MiCA or those providing crypto-asset services under MiCA without the need for registration.

The new rules impose specific obligations on:

- Reporting crypto-asset service providers, who must collect and verify information about crypto-asset

users following due diligence procedures and report relevant data to the competent authority for users residing in the EU, with certain exceptions.

- The competent authority in the Member State that receives the information must then transmit the reported data to the relevant authority in the Member State where the crypto-asset user is domiciled.

9. How can blockchain companies address data privacy and protection regulations in your jurisdiction, while ensuring transparency and security on decentralized networks?

Blockchain companies in Cyprus must navigate the complexities of complying with data privacy and protection regulations, particularly the General Data Protection Regulation (GDPR) and its national transposition through the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data 125(I)/2018, while preserving the core principles of transparency and security inherent in decentralized networks. The immutable and distributed nature of blockchain creates challenges in areas such as the right to erasure and identifying the responsible parties (data controllers and processors) under GDPR. To address these issues, companies must adopt privacy-centric designs, implement innovative technologies, and align their operations with both EU and Cyprus regulatory frameworks.

10. How do immigration policies, such as the U.S.'s H-1B and L-1 visas, impact the ability of fintech companies to hire international talent in your jurisdiction?

EU Citizens are free to engage in any economic activity, either as paid employees or self-employed persons, service providers under the same conditions as Cypriot citizens.

Non-EU Citizens must obtain a work permit, noting that a number of criteria need to be satisfied for the competent authority to issue the work permit, including that the employer was unable to find available local or EEA personnel for the relevant position.

On 15 October 2021, the Council of Ministers approved a new strategy aimed at attracting companies to establish or expand their operations in Cyprus, which came into effect on 2 January 2022 (the "New Strategy"). This strategy replaces the previous policy governing the employment of third-country nationals by foreign-interest

companies, introducing more flexible and business-friendly measures to support the hiring of skilled international talent.

Key provisions of the New Strategy include the removal of maximum quotas on foreign staff. Companies are now permitted to employ an unlimited number of highly paid third-country nationals. While the categories of Directors, Key Personnel, and Specialists remain in place for administrative and statistical purposes, the definition of "Specialists" has been expanded, removing restrictions on specific professions or skills. However, companies must commit to ensuring that 30% of their workforce consists of Cypriots or EU citizens within a five-year period, ending on 2 January 2027. Compliance with the 70:30 ratio will be reviewed at that time, with non-compliance cases evaluated on a case-by-case basis.

The employment of third-country nationals in companies of foreign interest is subject to compliance with applicable legislation as well as the requirements outlined in the New Strategy. Under this framework, employees in such companies are categorized as follows:

(a) Highly Paid Employment

This category applies to individuals receiving a minimum gross monthly salary of €2,500. Notably, third-country nationals who currently hold residence and employment permits under the BCS Key Personnel category, with a gross monthly salary of €2,000 or more, will be allowed to renew their permits with the same employer at the same salary level until 31 December 2026, without the need to increase their payroll.

To qualify, candidates must meet the following criteria:

Hold relevant academic qualifications or possess at least two years of experience relevant to the position.

Have an employment contract with a minimum duration of two years.

(b) Employment at the Supportive Level

For employment at the supportive level, a labour market test must be conducted, and the employment contract must be sealed by the Department of Labour to ensure compliance with the regulatory requirements.

This classification ensures that both highly skilled and supportive-level employment opportunities in companies of foreign interest are aligned with the legislative and strategic goals of attracting and retaining international talent.

In addition to the above the "Cyprus Digital Nomad Visa" has been introduced, with individuals that are granted with a Digital Nomad residence permit benefitting from the following:

- (a) Right of residence for a year in Cyprus, with a possibility of renewal for further two years.
- (b) Right of residence for family members, for the same period as the Digital Nomad, without the right to be employed or perform economic activity in Cyprus.
- (c) If they reside in the Republic for one of more periods that in total exceed 183 days within the same tax year, then they are considered tax residents of Cyprus, provided they are not tax residents in any other country.
- (d) Family members can reside in Cyprus for the same period as the Digital Nomad, however, without the right to be employed or perform any economic activity in Cyprus.

11. What are the key regulatory and compliance requirements that a fintech must address when entering the market in your jurisdiction, and how can the company ensure adherence to all applicable laws and regulations?

Fintech companies entering the Cyprus market must address a range of regulatory and compliance requirements to ensure adherence to local and EU laws. Key considerations include licensing, AML, consumer protection, data privacy, and taxation. Depending on their business model, companies may need authorization from CySEC or the CBC under frameworks such as, indicatively, MiCA, the Electronic Money Law, the Investment Services Law. Establishing robust governance structures and submitting comprehensive applications, including business and compliance plans, are essential first steps.

Compliance with the AML Law is critical, requiring fintech companies to implement strict AML policies, customer due diligence processes, and transaction monitoring systems. Similarly, adherence to GDPR mandates robust data protection measures, such as encryption and privacy-focused systems, to safeguard customer data. Companies must also ensure transparency in their services, fair treatment of consumers, and accurate financial reporting in line with applicable tax laws and EU directives like DAC6 and the upcoming DAC8. Partnering with local experts and maintaining open communication with regulators will help fintech companies navigate this regulatory landscape effectively and establish a compliant presence in Cyprus.

12. How should a fintech approach market entry strategy in your jurisdiction, considering factors such as target customer demographics, competitive landscape, and potential partnerships with banking and other financial institutions?

To successfully enter the Cyprus market, fintech companies should focus on understanding the local regulatory environment, and in this respect it is of the essence to engage local professionals to advise them on the local regulatory framework, including licensing requirements, data protection laws AML policies. The Innovation Hubs and Sandbox programs introduced by CBC and CySEC are good entry points and order to test the regimes in Cyprus.

Identifying target customer segments, such as the tech-savvy younger population and the growing number of SMEs seeking digital financial solutions, is key. The competitive landscape includes a mix of traditional banks modernizing their services and emerging fintechs, highlighting the need for a distinct value proposition. Strategic partnerships with local banks and payment service providers can facilitate trust and market penetration, while collaborating with Cyprus's fintech associations and leveraging the island's position as a regional business hub can accelerate growth.

13. What are the primary financial and operational risks associated with entering the market in your jurisdiction, and how can the fintech effectively mitigate these risks to ensure a smooth transition and sustainable growth?

Entering the Cyprus market presents risks such as navigating complex EU-aligned regulations, intense competition from established players, and potential cybersecurity threats. Fintechs can mitigate these by partnering with local professionals, leveraging collaborations with banks and payment providers, and focusing on underserved niches like SMEs or cross-border solutions. Prioritizing robust cybersecurity measures and establishing a local presence to access talent and market insights are also key. A gradual rollout, supported by early feedback, can help ensure a smooth transition and sustainable growth. Available sandbox programs may be of great value to start-ups in order to test their mode of operation in a small-scale regulated environment.

14. Does your jurisdiction allow certain business functions to be outsourced to an offshore location?

As a general approach outsourcing is permitted but companies must adhere to strict guidelines to ensure accountability, data protection, and operational resilience, however, each case will be considered on its own merits together with the regulator.

While outsourcing non-critical functions (e.g., IT support, customer service) is generally straightforward, outsourcing core activities requires careful planning, compliance with regulatory requirements, and often, the ability to justify that risks are adequately managed.

15. What strategies can fintech companies use to effectively protect their proprietary algorithms and software in your jurisdiction, and how does patent eligibility apply to fintech innovations?

Cyprus law affords protection to intellectual property rights such as trademarks, patents, industrial designs and copyrights.

Patents

Patent protection is afforded, pursuant to the Cyprus Patents Law (16(I)/1998), to inventions that satisfy the following criteria:

- (a) they are novel;
- (b) it is an inventive step; and
- (c) must have the potential to be used for industrial purposes.

Patents can be registered and protected domestically, at an EU level and internationally. It is noted that computer programs for Cyprus law purposes are not considered as patentable.

Industrial Design

This is an intellectual property rights which protects the visual appearance of a product or part of it. Such protection is afforded pursuant to the Industrial Designs and Models Law (4(I)/2002), noting that in order for design or model to be protected and registrable it must be novel and have an individual character.

Copyrights

Copyright is an automatic right protecting a broad range

of rights, including artistic work, software and computer programs. Provided that the criteria set out by the Copyright and Neighbouring Rights Law (59/1976) are met then copyright protection is afforded automatically without any prerequisite for registration.

16. How can a fintech company safeguard its trademarks and service marks to protect its brand identity in your jurisdiction?

Trademarks in Cyprus are afforded protection pursuant to the Trademark Law Cap. 268, and by virtue of a registration with the national competent authority. Protection can also be afforded at an EU or on international level pursuant to the following:

- the Paris Convention for the Protection of Industrial Property,
- the WIPO (World Intellectual Property Organisation) Convention,
- the Madrid Protocol,
- the Agreement on Trade-Related Aspects of Intellectual Property Rights.

17. What are the legal implications of using open-source software in fintech products in your jurisdiction, and how can companies ensure compliance with open-source licensing agreements?

Using open-source software in fintech products in Cyprus is legal but requires careful compliance with licensing agreements. Fintechs must review license terms to understand obligations, such as attribution or sharing modifications under certain licenses. Regular audits, clear policies on usage and tools to track compliance can help manage risks. It's also crucial to ensure GDPR compliance and cybersecurity standards to avoid data protection issues. Consulting legal experts ensures proper use and helps mitigate risks associated with intellectual property and licensing conflicts.

18. How can fintech startups navigate the complexities of intellectual property ownership when collaborating with third-party developers or entering into partnerships?

Fintech startups in Cyprus can navigate intellectual property complexities by establishing clear agreements and safeguards upfront. It is important for fintech companies to obtain advice and guidance from local

professionals in good time, and to register any intellectual property rights that are registrable.

When collaborating with third-party developers, startups should use detailed contracts that specify who owns the IP for any software, tools, or solutions developed. Typically, this involves including "work-for-hire" clauses or assigning full ownership of IP to the startup upon completion of the project.

For partnerships, startups should ensure that joint development agreements clearly define ownership rights, licensing terms, and usage restrictions for shared innovations. It's also important to conduct due diligence to ensure that any third-party contributions are free from pre-existing IP conflicts or restrictive licenses. Consulting with IP legal experts can help fintechs protect their proprietary technology and avoid disputes, ensuring long-term control over their innovations.

19. What steps should fintech companies take to prevent and address potential IP infringements, such as unauthorized use of their technology or brand by competitors?

Fintech companies should take proactive steps to prevent and address potential IP infringements. First, they should secure robust intellectual property protections by registering trademarks, patents, and copyrights for their technology, brand, and key innovations. Regularly monitoring the market for potential infringements, such as unauthorized use of their brand or technology, is also critical.

Well drafted contracts with employees, developers, and partners should include confidentiality and intellectual property related clauses to protect proprietary information. If an infringement is detected, fintechs should act quickly by seeking legal advice in order to safeguard their rights.

20. What are the legal obligations of fintechs regarding the transparency and fairness of AI algorithms, especially in credit scoring and lending decisions? How can companies demonstrate that their AI systems do not result in biased or discriminatory outcomes?

Fintech companies in Cyprus are subject to legal obligations around the transparency and fairness of AI algorithms, particularly in credit scoring and lending, as these activities align with EU regulations like the GDPR

and the AI Act. These laws emphasize accountability, fairness, and the prevention of bias in automated decision-making.

The AI Act, which entered into effect on August 1, 2024, marks the world's first legislative framework dedicated to regulating artificial intelligence. Its primary goal is to ensure that AI technologies created, implemented, and utilized within the EU are both safe and respectful of fundamental rights. The regulation emphasizes adherence to safety, transparency, and ethical standards before AI systems can be introduced or used in the market.

21. What are the IP considerations for fintech companies developing proprietary AI models? How can they protect their AI technologies and data sets from infringement, and what are the implications of using third-party AI tools?

Fintech companies in Cyprus developing proprietary AI models should focus on securing their intellectual property by protecting their algorithms through the appropriate registrations, if applicable. Clear agreements with developers and partners are essential to define ownership and usage rights. Regular monitoring for potential infringements and consulting IP legal experts can help safeguard their technologies and data.

22. What specific financial regulations must fintechs adhere to when deploying AI solutions, and how can they ensure their AI applications comply with existing financial laws and regulations? Are there specific frameworks or guidelines provided by financial regulatory bodies regarding AI?

Fintechs in Cyprus deploying AI solutions must comply with EU regulations, directives and local laws such as GDPR for data protection, the Payment Services Law, the Electronic Money Law, for secure and transparent financial services. Additionally, they need to adhere to AML Law requirements and the principles of fairness, accountability, and transparency outlined in AI Act.

23. What risk management strategies should fintech companies adopt to mitigate potential legal liabilities associated with AI technologies?

First of all, fintech companies should seek professional advice throughout their operations to ensure compliance

with applicable local and EU laws, regulations and directives. Additionally, they should regularly audit AI algorithms to identify and eliminate biases that could lead to discriminatory outcomes or unfair practices. Also, they should ensure that they have well-drafted contracts with clear liability clauses in agreements with developers, partners, and third-party providers to address ownership, licensing, and responsibilities.

24. Are there any strong examples of disruption through fintech in your jurisdiction?

While there isn't a single example that fully captures the scope of disruption, the transformations in the banking sector offer valuable insights. An increasing number of electronic money institutions and payment institutions are being licensed by CBC under the Electronic Money Law and the Payment Services Law. This trend reflects a positive shift toward more technology-driven banking services.

Additionally, the implementation of PSD2's open banking obligations has led to a rise in licensed Account

Information Service Providers in recent months. This development signals the growing momentum in Cyprus' fintech sector, with more initiatives likely to follow, further advancing the country's fintech landscape.

25. Which areas of fintech are attracting investment in your jurisdiction, and at what level (Series A, Series B, etc.)?

To date, the majority of fintech-related investments in Cyprus have focused on early-stage funding, ranging from pre-seed to Series A, as most investments originate from start-up companies. However, as Cyprus continues to establish itself as a fintech hub, we anticipate a shift toward more mature funding rounds, such as Series B and Series C investments.

Additionally, there is growing interest in ICOs and investments in innovative software solutions. We believe that the introduction of MiCA which will provide a clearer regulatory framework for the crypto industry in Europe, will further increase and accelerate the growth of crypto-related investments in Cyprus.

Contributors

Akis Papakyriacou
Managing Partner

akis@papakyriacoulaw.com

