FinTech in Portugal: overview

by Tiago Correia Moreira, Helena Correia Mendonça, José Miguel Carracho and David Paula, *Vieira de Almeida*

Country Q&A | Law stated as at 01-Mar-2021 | Portugal

A Q&A guide to FinTech in Portugal.

The Q&A provides a high-level overview of the financial services sector; the FinTech sector; regulatory environment for alternative finance activities, payment platforms, investment/asset management and InsurTech; regulatory compliance; government initiatives; cross-border provision of services and the future of FinTech.

Overview of financial services sector

1. What are the types of entities that form the financial services sector in your jurisdiction?

The financial services sector in Portugal consists of entities such as:

- Banks (including investment banks and mutual banks).
- Credit and mortgage credit institutions.
- Securities brokerage and advisory firms.
- Insurance companies.
- Payment and e-money institutions.
- Payment initiation service providers.
- Account information service providers.
- Crowdfunding platforms (either equity or debt-based) managing entities.

2. Which key regulatory authorities are responsible for the financial services sector?

Bank of Portugal (BoP)

The BoP is the financial services regulator responsible for the oversight and regulation of the banking and financial sector, notably banks, credit and mortgage credit institutions, and payment and e-money institutions.

Portuguese Securities Market Commission (CMVM)

The CMVM oversees all securities market-related business and activities (including crowdfunding platforms and all other traditional players and activities). The CMVM oversees jointly with the BoP securities market activities performed by entities that are regulated by the BoP.

Insurance and Pension Funds Authority (ASF)

The ASF is responsible for the supervision of the insurance and pension funds sector.

Overview of FinTech sector

3. What areas of the financial services sector has FinTech most significantly influenced?

Payments

Payments is an area of increased relevance, especially with the introduction of new solutions and platforms, such as MbWay. MbWay is a service by SIBS (the entity responsible for managing Multibanco, the intra-bank transfer and payments systems) which makes it possible to make instant transfers between bank accounts. Several major banks have also incorporated SIBS's service into their apps and mobile banking platforms. This payment method is now widespread and has been adopted by several retailers (either in the context of online shopping or in-person payments), widening the scope of MbWay from a fast and easy way to transfer funds between individuals into a significant payment method used in other types of transactions.

Crowdfunding

Crowdfunding is another area of the financial services sector that has been significantly influenced by FinTech. New crowdfunding players have entered the market after a rather long wait between the approval of the legal framework and the actual granting of licences by the CMVM. Crowdfunding businesses are starting to take off and the authors expect more new players to enter the market in the near future, as both investors and businesses have already started seeing this area as a real alternative to traditional equity and debt financing.

Payment services

The transposition of the Payment Services Directive (*(EU) 2015/2366*) (PSD2) into Portuguese law (mid-November 2018) has also paved the way for new businesses (and solutions from existing ones) to enter the payment initiation services and account information services markets in 2019 and 2020. This has been increased due to the growth of e-commerce and contactless and/or remote payments in the context of the novel 2019 coronavirus disease (COVID-19) pandemic.

Some companies (including banks) in Portugal have already launched account aggregation services that allow their customers to access their integrated bank account information held with other credit institutions, therefore engaging in direct competition with account information service providers licensed under PSD2. Additionally, SIBS, leveraging on its unique position in the Portuguese payments market, has launched SIBS API Market. SIBS API Market is a platform which 18 financial institutions take part in and which allows them to test their payment initiation and account information solutions, with the support of a specialised technical team. This enables access to, and full usage of, the SIBS API Market infrastructure.

PSD2 may enhance and further influence the FinTech ecosystem in Portugal, fostering the emergence of new players and businesses as well as business partnerships with, or acquisitions by, traditional stakeholders and incumbent firms.

4. How are traditional financial services firms engaging with FinTech?

The most common approach to FinTech by traditional financial services entities appears to be carried out either by internal development and R&D or by integrating outsourced services or solutions to tech firms.

Cross-firm collaboration between banks and solely-FinTech businesses is not very common. However, with the transposition of PSD2 into Portuguese law, new partnerships have started, and will probably continue, to arise, specifically with third-party providers (TPPs) rendering services to other financial firms (for example, in relation to open banking). These partnerships are leveraging on the increased digitisation of the banking sector, which has seen increased growth during 2020 due to the effects of the COVID-19 pandemic and the need for innovative products and services to reach the market quickly.

However, it is still unclear how open traditional financial services entities will be in matters such as open banking, as the recent trend in the Portuguese market has steered towards such services being provided by traditional banks (and not FinTech firms).

Regulatory environment

5. What regulatory initiatives have been introduced to support technology innovation and development in the financial services sector?

In 2020, the Portuguese Government approved Resolution of the Council of Ministers No. 29/2020, which establishes general principles for a legislative framework that promotes and facilitates research, demonstration and testing activities, in Technology Free Zones, of innovative technologies, products, services, processes and models. The Resolution goes beyond the creation of disparate "regulatory sandboxes", "innovation spaces", "experimental spaces" or "living labs" that are set up for specific sectors. It adopts a cross-sector and integrated approach for experimentation activities, therefore reducing burdens and promoting a culture of experimentation. The Portuguese Government is currently studying and drafting cross-sector and primary legislation for these Technology Free Zones, aiming to ensure a common vision for all sectors and areas of activity while reflecting the specificities of each sector and respective regulations, including for FinTech businesses. The Portuguese legislator and regulatory authorities' approach to FinTech had previously been somewhat neutral (due partly to the late transposition of PSD2 with a delay of almost a year from the deadline of 13 January 2018).

The Portuguese financial regulators (that is, the Bank of Portugal, the CMVM and the ASF) have implemented the Portugal FinLab programme to establish an easily accessible communication channel between entrepreneurs and emerging companies and the regulators. The programme is aimed at supporting the development of FinTech businesses and companies in navigating the legal and regulatory challenges. Additionally, the authors have noticed an increased interest by the regulators in these matters, as they have been actively participating in FinTech conferences and publishing relevant information on their respective websites.

Additionally, Portugal Fintech (a Portuguese association supporting the emerging FinTech ecosystem) continues to promote the Portuguese FinTech market, by promoting the visibility of FinTech, RegTech, InsurTech and cybersecurity companies in their early stages with the legislator, other start-ups, investors, consultants, banks, regulators and other relevant entities. Portugal FinTech also opened the FinTechHouse in late 2019, which aims to be a technological innovation and financial services hub and is described as "a unique place that aims to be the meeting point of the entire ecosystem". Portugal FinTech also recently launched the Fintech365 programme to help companies to better navigate the regulatory challenges faced by the financial sector and accelerate their digital transformation

Alternative finance

6. How is the use of FinTech in alternative finance activities regulated?

Alternative finance activities are regulated at a national level under the crowdfunding legal framework and are under the CMVM's regulatory supervision.

Crowdfunding is regulated by Law No. 102/2015 of 24 August 2015. Law No. 3/2018 of 9 February 2018 sets out the sanctions for violation of Law No. 102/2015.

This regime is complemented by CMVM Regulation No. 1/2016, which further sets out the application requirements and the procedures for obtaining and maintaining a valid licence to operate a crowdfunding platform (either equity or debt).

Before they can start operating, crowdfunding firms must register with, and be authorised by, the CMVM. As part of the application, certain documents must be included, such as:

- Corporate details.
- Structure and beneficial ownership.
- Managers' identification and fit and proper documentation.
- Business plan and model.
- Indication on whether the firm should be considered a financial intermediary or an agent of a financial intermediary.
- Evidence of compliance with the minimum financial requirements. After registration, these minimum financial requirements must be either:
    - a minimum share capital of EUR50,000;
    - an insurance policy covering at least EUR1 million per claim, and at least EUR1.5 million in aggregate claims per year; or
    - a combination of both that ensures sufficient similar coverage.

Further developments may arise in this field following the entry into force of the Crowdfunding Regulation (*(EU) 2020/1503*) on 10 November 2021. As the market develops and the number of market players increases, P2P funding alternatives offered by crowdfunding platforms will become more sophisticated in the medium to long term.

Payment platforms

7. How has FinTech resulted in innovations to payment services and how is it regulated?

The regulatory treatment of FinTech in Portugal greatly depends on the exact legal nature of the products and services the FinTech company is offering.

The main legal and regulatory concerns in terms of FinTech are those relating to payment services and e-money related activities, as well as crowdfunding platforms (*see Question 6*).

The two current main categories of FinTech companies are payment services institutions and e-money issuers. They are both regulated under Decree-Law No. 91/2018 of 12 November 2018, containing the Payment Services and E-Money Legal Framework (PSEMLF), which transposed PSD2 into Portuguese law.

The PSEMLF also set out the requirements for payment initiation service providers (PISPs) and account information service providers (AISPs) to enter the Portuguese market.

Investment/asset management

8.How is the use of FinTech in the retail investment market regulated?

The securities market is regulated by the Portuguese Securities Code, enacted by Decree-Law No. 486/99 of 13 November 1999 (as subsequently amended and currently in force), which incorporates the changes resulting from the Markets in Financial Instruments Directive (*2014/65/EU*) (MiFID II).

There are currently no specific regulations on the use of FinTech in the securities market. All securities market-related activities are subject to the existing securities framework for traditional entities and activities (if they fall within their scope).

Some FinTech matters (such as blockchain and cryptocurrencies) are still outside the scope of securities laws altogether. The CMVM does not regulate cryptoassets and initial coin offerings (ICOs) unless they qualify as securities (*see Question 14*).

9. How is the use of FinTech in wholesale securities markets regulated?

There are currently no specific regulations on the use of FinTech in wholesale securities markets (*see Question 8*).

InsurTech

10. How is the use of FinTech in the insurance sector regulated?

InsurTech activities are not specifically regulated. They are regulated by the ASF at national level under the same framework as traditional insurance activities. However, the ASF is actively engaged in InsurTech developments and open to new initiatives in this respect (notably through the Portugal FinLab programme (*see Question 5*)).

On a national level, insurance and reinsurance activities are governed by the Insurance Legal Framework, approved under Law 147/2015 of 9 September 2015, which sets out the requirements for authorisation and registration of all insurance companies operating in Portugal, as well as for their prudential supervision.

InsurTech solutions and services are generally accepted in the Portuguese market, provided they comply with the general insurance and reinsurance legal framework.

Cryptoassets

11. What is the legal status of cryptoassets?

Cryptoassets currently have no specific legal status. The legal status of cryptoassets varies depending on their specifications and the rights and obligations of holders (which may qualify them as securities, electronic money or virtual assets).

In relation to cryptocurrencies, the consistent current regulatory approach in Portugal has been to not consider cryptocurrencies as legal tender and to not issue specific regulation dealing with them. Both the BoP and the CMVM follow this approach.

12. How are cryptoassets regulated?

There are currently no specific regulations on cryptoassets.

The BoP has (as far back as 2013) issued a clarification stating that Bitcoin (and all other cryptocurrencies) cannot be considered secure currency, as:

- It is issued by unregulated and unsupervised entities.
- Users bear all the risks (as there is no fund for the protection of depositors/investors).

This approach closely follows the position of the European Banking Authority (EBA). Specific regulation on cryptocurrencies is not expected soon, as both the Portuguese Government and the BoP have stated that they will not unilaterally regulate cryptocurrencies, and that the first step will be taken by the European Commission.

In this respect, both the European Securities and Markets Authority (ESMA) and EBA sent reports on 9 January 2019 to EU policymakers on ICOs and cryptoassets assessing the applicability and suitability of EU legislation in relation to these and advising the European Commission. According to the EBA's report, the competent national authorities report low cryptoassets activity levels in their jurisdictions and that it is not currently a threat to financial stability. However, in particular with regard to consumer protection, market integrity and the level playing field, the report flags the following issues:

- Current EU financial services legislation does not apply to a number of forms of cryptoasset/activity.
- Specific services relating to providing cryptoasset custodian wallets and cryptoasset trading platforms are not considered regulated activities under EU law.
- Different approaches are emerging across the EU.

The EBA therefore recommends that the European Commission carries out a cost/benefit analysis to assess whether EU-level action to address these issues is appropriate and feasible at this stage.

ESMA has also identified a number of concerns in the current financial regulatory framework regarding cryptoassets (according to the press release for ESMA's report). These gaps and issues fall into two categories:

- For cryptoassets that qualify as financial instruments under MiFID, some areas require potential interpretation or reconsideration of specific requirements to allow for an effective application of existing regulations.
- For cryptoassets that do not qualify as financial instruments, the absence of applicable financial rules leaves investors exposed to substantial risks. At a minimum, ESMA considers that anti-money laundering (AML) requirements should apply to all cryptoassets and related activities. There should also be appropriate risk disclosure in place, so that consumers are made aware of the potential risks before committing funds to cryptoassets.

ESMA therefore recommends that the European Commission either:

- Proposes a bespoke regime for specific types of cryptoassets (such as tokens, which do not qualify as financial instruments) by means of a directive, allowing for the tailoring of the rules to the specific risks and issues.
- Does nothing (which would fail to address the known investor protection and market integrity concerns).

Despite the lack of regulation and supervision, the BoP has indicated that the use of cryptocurrencies is not forbidden or illegal. Therefore, the BoP is currently more focused on a preventive and educational approach, by alerting to the risks of cryptocurrencies.

The CMVM has also issued an alert to investors in November 2017 on ICOs indicating that most ICOs are not regulated. This effectively means that investors are unprotected from the following:

- High volatility/lack of funds.
- Potential of fraud/money laundering.
- Inadequate documentation (most ICOs have no prospectus, only a "white paper", which is only a marketing document and not legally binding).
- Risk of loss of the invested capital.

The CMVM still paved the way for regulation according to the specific circumstances of the ICOs.

Considering the above, the usual distinction between the different types of tokens (or the rights and obligations which their issuance and possession entail) underlying the transactions may prove useful. If tokens are used mainly as a means of payment, the regulatory approach of the BoP and EBA is the relevant one. Conversely, where tokens are more similar to securities, the approach of the CMVM/ESMA is the applicable one.

However, some progress appears to have been made at EU level with the digital finance package, which includes proposals for a:

- Regulation on markets in cryptoassets (*COM/2020/593 final*) (MiCA).
- Regulation on a pilot regime for market infrastructures based on distributed ledger technology (*COM(2020) 594 final*).

13. Have specific anti-money laundering measures been introduced in relation to cryptoasset activities?

Law 58/2020 of 31 August 2020 transposed the recent AMLD changes, extending the scope of application of the Portuguese AML framework to entities engaged with providing services in cryptoassets (namely, to crypto exchanges and wallet providers offering custodial services). These must now:

- Register with the BoP.
- Comply with know-your-customer (KYC) and AML procedures for transactions taking place in their exchanges or wallets. For example, they must submit all relevant documentation and statements of responsibility of members of their board of directors, supervisory boards and senior management.

Additionally, general rules on AML and terrorism financing apply to cryptoasset activities and any business involving virtual assets (other than those qualifying as electronic currency, which fall under the regulation of the PSEMLF).

Distributed ledger technology solutions

14. How is the use of blockchain in the financial services sector regulated?

There are no specific regulations on the use of blockchain or, in general, of distributed ledger technologies (including in the financial sector).

Despite the lack of regulatory framework for blockchain itself, services resorting to smart contracts seem to have some legal comfort. The E-Commerce Law (Decree-Law No. 7/2004) includes a specific provision dealing with contracts automatically executed by means of computers without human intervention. This states that contract law applies to these types of contracts as well as programming errors, malfunctions and distorted messages.

While self-executing or smart contracts are a step further from contracts concluded without human intervention, it appears that they are permitted under Portuguese law. The abovementioned provision may apply to them. There is a general principle under Portuguese law that contracts are not subject to a specific form unless otherwise provided. However, no specific legal framework exists in relation to smart contracts.

However, the authors expect that any further legal regulation on a national level may be delayed until the adoption of the proposed Regulation on a pilot regime for market infrastructures based on distributed ledger technology (*COM(2020) 594 final*).

Additionally, the European Blockchain Partnership is planning to launch a pan-European blockchain regulatory sandbox for 2021/22 to test blockchain solutions, including in areas such as data portability, B2B data spaces, smart contracts, and digital identity, in the health, environment, mobility, energy and other key sectors.

Financial services infrastructure

15. What types of financial services infrastructure-related activities of FinTech businesses are regulated?

Generally, there is no specific regulation of the infrastructure and technologies underlying the FinTech sector. However, there are rules addressing aspects of FinTech services with infrastructural impact, such as those relating to security requirements, notably:

- The PSEMLF.

- Regulation (EU) 2018/389 supplementing PSD2 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Regulatory Technical Standards Regulation).

The PSEMLF requires payment service providers to have appropriate mitigation measures and control mechanisms to manage operational and security risks. As part of this, payment service providers must establish and maintain effective incident management procedures (including for the detection and classification of major operational and security incidents).

Providers must also:

- Implement strong customer authentication mechanisms (that is, with at least two independent authentication elements (such as password and fingerprint)), a requirement further developed in the Regulatory Technical Standards Regulation.
- Ensure the confidentiality and integrity of the personalised security credentials of their payment service users (including authentication codes) during all phases of the authentication.
- When accessing the Application Programming Interfaces (APIs) of banks, identify themselves with the banks (or account servicing payment service providers).

In this context, the Regulatory Technical Standards Regulation establishes that payment service providers must use qualified certificates for either:

- Electronic seals (*Article 3(30), Electronic Identification Regulation (910/2014)*).
- Website authentication (*Article 3(39), Electronic Identification Regulation*).

The provision of payment services requires robust and secure infrastructures. For example, PSD2 requires access to the services of technical infrastructures of payment systems to be subject to appropriate requirements (to ensure the integrity and stability of those systems).

Another key issue is customer due diligence (*see Question 16, Anti-money laundering*). FinTech companies that qualify as payment or electronic money institutions can (similarly to traditional banks) resort to customer identification via video conference with the customer or via trust service providers (within the meaning of the Electronic Identification Regulation), in accordance with BoP Notice 2/2018. Several technical requirements must be met, such as that the video conference takes place in real time and without interruptions or pauses (these requirements must be reflected in the procedures of the payment or electronic money institutions).

Regulatory compliance

16. What are the key regulatory compliance issues faced by FinTech businesses?

FinTech businesses are subject to legal regimes that go beyond the ones specific to the financial sector. This is the case, for example, of data protection, cybersecurity and consumer protection. In addition, regulatory requirements for licensing, banking secrecy rules and AML provisions also apply.

Data protection

FinTech businesses collect, control and process vast amounts of personal data (including KYC data) and are therefore subject to data privacy rules.

These rules are those provided in the GDPR. The GDPR applies not only to FinTech companies established in the EU, but also to companies established outside the EU if:

- They have customers in the EU.
- The processing of customers' personal data is made in the context of the offering of services to those data subjects (regardless of whether a payment is required from the data subjects).

The European Data Protection Board (EDPB) has clarified that the intention to target customers in the EU is key to assess whether entities established outside the EU are subject to the GDPR (according to its Guidelines 3/2018 on the territorial scope of the GDPR).

The processing of personal data by FinTech companies may require customer consent. If that is the case (notably, if the processing of a customer's personal data is not strictly necessary to provide a payment service expressly requested by a payment service user, as the EDPB clarified in its PSD2 Letter to Sophie in't Veld from 5 July 2018), pre-ticked opt-in boxes will no longer be allowed for obtaining valid consent. This is because consent must be expressed either through a statement or by a clear affirmative action.

The GDPR places onerous accountability obligations on data controllers (such as payment service providers that are regulated under PSD2) to demonstrate compliance, which is a major paradigm shift in the data protection regime. This includes:

- Conducting data protection impact assessments (DPIAs) for more risky processing operations (such as those involving the processing of personal data that may be used to commit financial fraud).
- Notifying personal data breaches to the Portuguese Data Protection Authority through its online form.
- Implementing data protection safeguards by design and by default.

Another important aspect of data processing in the context of FinTech business is the definition of clients' profiles and business segmentation, as well as automated decision-making based on profiling. Automated decisions are generally prohibited if they produce effects concerning the data subject or that significantly affect them and are based solely on automated processing of data intended to evaluate certain personal aspects relating to them.

The GDPR has introduced new provisions to address the risks arising from profiling and automated decision-making. The GDPR allows this type of decision-making only if the decision is either:

- Necessary for the entry into, or performance, of a contract or authorised by EU or member state law that applies to the controller. In this regard, the EDPB Guidelines 2/2019 on the processing of personal data

under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects make clear that controllers must assess what processing of personal data is objectively necessary to perform the contract.

- Based on the individual's explicit consent.

Where one of these grounds applies, additional safeguards must be introduced, and specific information must be disclosed about the automated individual decision-making (including profiling). Where automated decisions are being made about customers/data subjects, FinTech companies (as data controllers) must ensure the customers' rights to obtain human intervention, to express their point of view and to contest the automated decisions.

There are additional restrictions on using special categories of data (such as health-related data or biometric data) for any processing of personal data, which can ultimately have an impact on the way FinTech companies will implement strong customer authentication mechanisms under the Regulatory Technical Standards Regulation, as this Regulation suggests the use of payment service users' biometric data in that context.

There are also other data subjects involved in payment transactions and whose processing of personal data must be justified. For example, a silent party is a data subject who is not the user of a specific payment service provider, but whose personal data are processed by that specific payment service provider for the performance of a contract between the provider and the payment service user. For example, when a data subject A uses a payment service provider to make a payment to data subject B, data subject B is a silent party. According to the EDPB Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR, the processing of silent party data should be based on the controller and third party's legitimate interests to perform the contract with the payment service user. In addition, EDPB points out that effective and appropriate measures must be taken to ensure that reasonable expectations of silent parties are respected.

Without prejudice to the above, the Portuguese law implementing the GDPR (Law No. 58/2019, of 8 August) brings some additional adjustments or restrictions to the rules set out in the GDPR (notably regarding requirements for allowing the portability and interoperability of financial data, which will take place, whenever possible, in an open format).

The Portuguese Data Protection Authority (*Comissão Nacional de Protecção de Dados*) (CNPD) has consistently ruled that financial data is sensitive data (in the sense that it reveals aspects of individual private life) and should therefore be protected under the Portuguese Constitution, which may ultimately affect how Portuguese courts will apply the GDPR rules in respect of such financial data. In this context, the EDPB Guidelines 6/2020 note that it is highly likely that financial transactions can reveal special categories of personal data, and so payment service providers are advised to carry out a DPIA to map out and categorise what types of personal data they will be processing.

Additionally, the Free Flow Data Regulation (*(EU) 2018/1807*) (applicable since 29 May 2019) applies to all data other than personal data (as defined in the GDPR). This may include, in some instances, financial data processed by payment service providers (as clarified in Annex 5 to the European Commission's Impact Assessment Report on the Regulation). Under the Free Flow Data Regulation, the European Commission will encourage and facilitate the development of self-regulatory codes of conduct at EU level to contribute to a competitive data economy, based on the principles of transparency and interoperability. Specifically, these include the following:

- Best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format.
- Minimum information requirements to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information regarding the

processes, technical requirements, time frames and charges that apply if a professional user wants to switch to another service provider or port data back to its own IT systems.

Cybersecurity

Law No. 46/2018 of 13 August 2018 transposes the Cybersecurity Directive (*(EU) 2016/1148*) into Portuguese law. A FinTech company may be subject to the requirements of this law as an operator of essential services, especially if:

- It decides to register itself with the BoP as a credit institution (as defined in Article 4(1) of the Capital Requirements Regulation (*575/2013*)) or is a manager or operator of trading platforms, and is further identified as a provider of essential services by the National Cybersecurity Centre.
- It falls under the definition of digital service provider. The Cybersecurity Directive defines "digital service" as an "information society service" (which is defined in Article 1(1)(b) of Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification)). An information society service is:
    - an online marketplace (that is, a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace);
    - an online search engine; or
    - a cloud computing service (that is, a digital service that enables access to a scalable and elastic pool of shareable computing resources).

FinTech businesses that fall under one of these definitions must:

- Implement adequate security measures in their networks or information systems.
- Notify any security incidents they suffer to the National Cybersecurity Centre, taking into account the:
    - number of users affected by the incident, in particular users relying on the service for the provision of their own services;
    - duration of the incident;
    - geographical spread with regard to the area affected by the incident;
    - extent of disruption of the service (for digital service providers); and
    - extent of the impact on economic and societal activities (for digital service providers).

Non-compliance with Law No. 46/2018 may result in fines ranging from EUR1,000 to EUR50,000.

Additionally, the BOP Instruction No. 1/2019 of 15 January 2019 created an obligation to notify severe incidents related with the provision of payment services under PSD2. The Instruction applies to payment service providers

registered and authorised by the BoP. Instruction No. 21/2019 of 25 November 2019 regulates the notification of cybersecurity incidents.

Further developments are expected in the context with the new *EU Cybersecurity Strategy* presented by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy on 16 December 2020, which aims to address three areas of action:

- Resilience, technological sovereignty and leadership.
- Operational capacity to prevent, deter and respond.
- Co-operation to advance a global and open cyberspace.

The strategy also includes a proposal for a Directive on measures for a high common level of cybersecurity across the EU (NIS 2 Directive) (*COM/2020/823 final*).

Relevant EU legislative developments also include proposals for a:

- Regulation on digital operational resilience for the financial sector (*COM/2020/595 final*) which is focused on ICT risks and aims to provide clarity on the application of the NIS Directive in the financial sector.
- Directive on the resilience of critical entities (*COM/2020/829 final*), which aims to support member states in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents.

Consumer protection

FinTech businesses that provide services to consumers must comply with the Consumer Law. For example, information to the consumer must be provided in Portuguese.

Decree-Law 95/2006 of 29 May 2006 also sets out requirements that are aimed at consumer protection. When a distance contract relating to the provision of financial services is concluded with a consumer, certain information must be provided to the consumer (such as informing them of the right of withdrawal).

Licensing requirements

Payment institutions and electronic money institutions in Portugal must be authorised by the BoP before they can operate. The BoP issues licences on a case-by-case basis after an application is submitted and in accordance with the PSEMLF.

A company that is looking to obtain funding via equity or debt-based crowdfunding intermediation cannot do so without prior registration with the CMVM. Alternatively, for a company that is looking to obtain funding via donation or reward-based crowdfunding platform management, prior notification to the Portuguese Consumer General Directorate (*Direção Geral do Consumidor*) is required.

Banking secrecy

Article 1 of the PSEMLF extends banking secrecy obligations to payment service providers (and to their agents, workers and representatives), even if they are not credit institutions or financial institutions according to national law. Breaching banking secrecy rules is a criminal offence.

Bank secrecy rules determine that the disclosure of clients' data protected by bank secrecy (including cross-border transfers) is only permitted with prior customer authorisation or if the processing is necessary to ensure one of the following:

- Compliance with a legal obligation of the data controller.
- The performance of a task carried out in the public interest.

The CNPD has already ruled that all personal data processed by a bank is subject to bank secrecy.

When processing clients' data for the purposes of AML reporting, the disclosure of specific relevant personal data is based on the fulfilment of a legal obligation. It is therefore not necessary to obtain clients' authorisation for disclosure to the competent authorities.

The concept of "client authorisation" under the PSEMLF and the financial institutions legal framework differs from the concept of "consent" under the GDPR (that is, the inclusion of client authorisation provisions is part of and requisite of the services being provided by financial institutions, and can be included in general terms and conditions, whereas the consent is for GDPR purposes and must be based on an affirmative and explicit action by the client). Therefore, many banks and other financial institutions choose to collect clients' authorisation to disclose information covered by banking secrecy in the context of their general client terms and conditions.

Anti-money laundering

FinTech companies that are authorised as payment institutions under the PSEMLF and those that fall under the definition of electronic money institutions are bound by Law No. 83/2017 of 18 August (which transposes the Fourth Anti-Money Laundering Directive).

Under the Portuguese AML framework, these FinTech companies must (among others):

- Apply customer due diligence.
- Report suspicious transactions.
- Store copies of, or the extracted data from, documents supplied by customers in the context of customer due diligence.
- Store customer correspondence and any internal or external documents, records and analysis which show AML compliance.
- Implement adequate internal policies, procedures, controls and training to prevent money laundering.

AML obligations for entities managing crowdfunding platforms (regulated under Law No. 102/2015 of 24 August 2015) are less stringent. These entities must only store records of the:

- Complete identification of investors and beneficiaries.

- Amounts invested (segregated by investor and operation).
- Complete identification of persons who undergo partial or full depreciation of investments.
- Amounts of each investor's remunerations, share capital, dividends and profits.
- Complete identification of beneficiaries and donors, and the donated amounts per donor and per operation, for reward-based and donation-based crowdfunding.

Many compliance issues faced by FinTech businesses relate to uncertainty in terms of the applicable laws and regulations. The amount of applicable regulations and associated costs can be substantial (and may greatly differ depending on the type of business activity performed by the FinTech business). If this activity requires a licence or authorisation from the regulatory authorities, the procedures to obtain these are usually long and costly. Most times, this means that the company cannot operate until it has a licence or authorisation, which causes many firms (notably start-ups) to either go bankrupt, get bought or try to find another (more FinTech-friendly) jurisdiction to base their operations in.

FinTech firms may also struggle with the stringent AML (*see above*) and KYC laws and regulations, which sometime put too much strain on an early-stage firm's operations. This may also be aggravated by the data privacy and cybersecurity laws and regulations that may affect the FinTech business, especially if it is targeting the consumer market.

Despite this, the regulatory challenges faced by FinTech companies are beginning to be addressed and partially smoothed out, notably with the regulators being more approachable and sensible to the concerns of start-ups. A specific example is the promotion of initiatives such as Portugal Finlab (*see Question 5*).

17. When traditional financial services firms and FinTech firms enter into partnerships or other arrangements, what are the key legal, regulatory and practical issues they need to consider?

Most traditional financial services providers develop their own FinTech-related initiatives and can circumvent barriers, as the banking licence they have allows them to pursue most FinTech activities.

However, traditional financial services firms and FinTech firms enter into partnerships or other arrangements, the key issues that the parties consider are:

- Data protection and data sharing.
- Client ownership.
- Protection of client funds (where applicable).
- Compliance with AML obligations.
- Ownership of technology and partnership's goodwill.

- Service level agreements and associated penalties.

On 25 February 2019, the EBA published its revised Guidelines on Outsourcing Arrangements (EBA/GL/2019/02). The guidelines entered into force on 30 September 2019 and were made applicable in Portugal on 31 May 2020 by the BOP Circular Letter no. CC/201900000065. The CEBS Guidelines of 2006 (GL02/2006) on outsourcing and the EBA's recommendation on outsourcing to cloud service providers were repealed at the same time. FinTech companies that are investment firms under MiFID II, credit institutions, payment service providers and electronic money institutions must:

- Set up a comprehensive outsourcing framework (including outsourcer due diligence, oversight and audits, and contract management).
- Enter into (or review the existing) appropriate arrangements with outsourcers (including SLAs).
- Maintain an outsourcing register with all outsourcers and outsourced activities.

The Guidelines require those institutions to devote particular attention to outsourcing agreements that relate to critical or important functions, especially if the outsourcing concerns functions related to core business lines and critical functions (as defined in Article 2(1)(35) and 2(1)(36) of the Bank Recovery and Resolution Directive (*2014/59/EU*) (BRRD) and identified by institutions using the criteria in Articles 6 and 7 of Regulation (EU) 2016/778). For example, outsourcing agreements must include rules on sub-outsourcing of those critical or important functions (*section 13.1, Guidelines*).

When assessing whether an outsourcing arrangement relates to a function that is critical or important, institutions and payment institutions must take into account (together with the outcome of the ordinary risk assessment outlined in section 12.2 of the Guidelines) at least the following factors:

- Whether the outsourcing arrangement is directly connected to the provision of banking activities or payment services for which they are authorised.
- The potential impact of any disruption to the outsourced function or failure of the service provider to provide the service at the agreed service levels on a continuous basis on their:
    - short- and long-term financial resilience and viability, including (if applicable) their assets, capital, costs, funding, liquidity, profits and losses;
    - business continuity and operational resilience;
    - operational risk, including conduct, information and communication technology (ICT) and legal risks;
    - reputational risks; and
    - where applicable, recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation.
- The potential impact of the outsourcing arrangement on their ability to:
    - identify, monitor and manage all risks;
    - comply with all legal and regulatory requirements; and

    - conduct appropriate audits regarding the outsourced function.

- The potential impact on the services provided to its clients.
- All outsourcing arrangements, the institution's or payment institution's aggregated exposure to the same service provider and the potential cumulative impact of outsourcing arrangements in the same business area.
- The size and complexity of any business area affected.
- The possibility that the proposed outsourcing arrangement may be scaled up without replacing or revising the underlying agreement.
- The possibility to transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable, both contractually and in practice, including the estimated risks, impediments to business continuity, costs and time frame for doing so (substitutability).
- The ability to reintegrate the outsourced function into the institution or payment institution (if necessary or desirable).
- The protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the institution or payment institution and its clients, including compliance with the General Data Protection Regulation (*(EU) 679/2016*) (GDPR).

Unregulated FinTech companies (that is, providers of services to institutions who distribute their services to EU branches) must still observe certain outsourcing requirements, such as:

- Complying with the industry's regulatory standards (such as ISAE 3000 or ISAE 3402).
- Have a sub-outsourcing framework agreement.
- Entering into outsourcing agreements with sub-outsourcing providers.

Under the Guidelines, outsourcing means an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself.

18. Do foreign FinTech entities intending to provide services in your jurisdiction encounter regulatory barriers that are different from domestic FinTech businesses?

Foreign entities face the same regulatory issues as domestic FinTech businesses. The right to passport financial services in the EU and the freedom to provide services in the EU framework apply to payment and e-money institutions under the PSD2 regime.

19. What steps can be taken in your jurisdiction to protect FinTech innovations and inventions?

Protection of FinTech technology can take place by various means. The protection of software seems to be the most relevant, as FinTech technology usually relates to computer systems and applications. Software is protected in Portugal under the same legal rules that apply to copyright protection (according to Decree-Law No. 252/94 of 20 October 1994, as amended).

Copyright

Copyright does not require registration to arise, although works can be registered with the General-Inspection for Cultural Activities (IGAC).

Patents

Software itself cannot be protected by a patent, unless it meets the criteria to be considered a computer-implemented invention (that is, an invention whose implementation involves the use of a computer, computer network or other programmable apparatus). Computer-implemented business models can also be patented, to the extent that they are claimed as a technical solution for a technical problem (for example, automating a response considering the data collected) and involve technical considerations (for example, the reading of the database). Otherwise, business models are not patentable. A case-by-case analysis is necessary to determine if protection by patent is feasible.

Trade secrets

Technology developed in the context of a FinTech business can also be protected as a trade secret. Trade secrecy protects against any act of someone that assesses, appropriates or copies (or any other conduct that is considered contrary to honest commercial practices in the specific circumstances), without consent, information that:

- Is secret.
- Has commercial value due to its secrecy.
- Has been subject to reasonable steps to keep that information secret (for example, by entering into non-disclosure agreements) by the person lawfully in control of the information.

Current national legal provisions on trade secrecy (which are included in the Industrial Property Code, approved by Decree-Law No. 110/2018 of 10 December 2018) have been subject to considerable revision and expansion, which is mostly related to the transposition of the Trade Secrets Directive (*(EU) 2016/943*). The Trade Secrets Directive substantially changed the trade secrecy regime, specifically the protection criteria and enforcement regime.

Government initiatives to support FinTech

20. To what extent has the government in your jurisdiction sought to create a more favourable regulatory environment for FinTech businesses?

To date, no specific measures such as regulatory sandboxes or other incentives have been created for FinTech firms specifically.

However, Resolution of the Council of Ministers no. 29/2020 of 21 April 2020 establishes a set of principles for the creation of Technological Free Zones. The objective is to promote and facilitate research, demonstration and testing activities, in a real-life environment, of innovative technologies, products, services, processes and models. The Resolution notes the importance of adopting a legal framework that promotes and streamlines experimentation activities in a cross-sector manner to take advantage of all the opportunities brought by new technologies. This approach goes beyond the creation of disparate "regulatory sandboxes", "innovation spaces", "experimental spaces" or "living labs" that are set up by sector or for pre-defined fields. The Resolution further adds that the legal framework to be approved should take into account, for example:

- Legal flexibilisation (such as exception or experimentation regimes), whenever possible.
- Incentives for experimentation (such as regulatory sandboxes).

In addition, various initiatives are being promoted that can support FinTech businesses (*see Question 5 and Question 22*).

21. Are there any special regimes in place to facilitate access to capital for FinTech businesses?

There are no special regimes to facilitate access to capital for FinTech businesses. However, there are tax incentives for investors in start-ups. Investors in FinTech start-ups can therefore also benefit from them.

For example, *Programa Semente* for seed investors establishes that individual taxable persons who make eligible investments of up to EUR100,000 in start-ups can deduct 25% of the investment made from their taxable income (up to a limit of 40% of the total personal income tax due).

22. Is the government taking measures to encourage foreign FinTech businesses to establish a domestic presence?

The authors are not aware of specific measures targeted at foreign FinTech businesses. However, in the last few years, there have been incentives for the tech sector as a whole. The Portuguese Government is promoting the WebSummit in Portugal for the next few years and there are other measures aimed at encouraging start-ups and other tech firms to base their businesses in Portugal.

Other government initiatives include the Startup Portugal Programme, which is a four-year plan aimed at the early development of emerging start-ups and the creation of an incubator network for start-ups and entrepreneurs.

Additionally, although not directly related to the government itself, the creation of Portugal FinLab has greatly improved the approach of financial regulators to the FinTech ecosystem and is the result of a partnership between Portuguese FinTech companies and the BoP, CMVM and ASF. Under the FinLab initiative, entrepreneurs engage directly with the regulators and can receive an opinion about the regulatory issues that may arise from the implementation of their projects in a more informal and business-friendly fashion.

Cross-border provision of services

23. Are there any special rules that affect the cross-border provision of financial products or services by both domestic and foreign FinTech businesses?

Other than the general rules applicable under national and EU law to either national or foreign entities regarding cross-border payments and the provision of financial services, there are no FinTech-specific regulations in place.

The future of FinTech

24. What regulatory measures or initiatives may affect FinTech in your jurisdiction in the future?

The transposition of PSD2 into Portuguese law is still quite recent and its effects may only begin to be noticed in the near future. The authors therefore envisage that ancillary regulation from the BoP or the CMVM may be adopted in the next year to address any specific issues that may occur during the market's adaptation to the PSD2, with new

players emerging (notably TPPs) and starting to interact with established market participants. However, certain initiatives have started to arise and should bring new products and services to the market in the near future.

On a national level, the Portuguese initiative for the creation of Technological Free Zones (*see Question 20*) may also greatly encourage FinTech innovations and services in Portugal. This initiative may lay the foundations for regulatory sandboxes and provisional regulatory frameworks more suited to beta testing services and early-stage companies.

The proposed MiCA and Blockchain Regulations will also be a catalyst for further innovation and developments in the Portuguese FinTech market. Several traditional market players are starting to look into it as a means to develop new financing sources and solutions for their clients.

Contributor profiles

Tiago Correia Moreira, Partner

Vieira de Almeida
T + 351 213 113 677
F + 351 213 113 406
E *tcm@vda.pt*
W *www.vda.pt*

Professional qualifications. Lawyer, Portugal

Areas of practice. Banking and financial sectors, particularly the acquisition and sale of non-performing loans and secured loans (including aeronautic financing); all regulatory work pertaining to these sectors.

Languages. English, French

Professional associations/memberships. Admitted to the Portuguese Bar Association.

Helena Correia Mendonça, Principal Consultant

Vieira de Almeida
T +351 213 113 487
F +351 213 113 406
E *hcm@vda.pt*
W *www.vda.pt*

Professional qualifications. Lawyer, Portugal

Areas of practice. Information, communication and technology; aviation, space and defence; emerging technologies (including distributed ledgers/blockchain, robotics and AI); implementation of e-commerce platforms and websites; FinTech (mobile payments, payment services and e-money).

Languages. English

Professional associations/memberships. Admitted to the Portuguese Bar Association; member of APDC - Portuguese Association for the Development of Communications.

José Miguel Carracho, Associate

Vieira de Almeida
T +351 213 113 677
F +351 213 113 406
E *jmc@vda.pt*
W *www.vda.pt*

Professional qualifications. Lawyer, Portugal

Areas of practice. Banking and financial sectors (particularly the acquisition and sale of non-performing loans and secured loans); FinTech and payment services matters, and blockchain/DLT (payment and e-money institutions, as well as crowdfunding platforms).

Languages. English, Spanish

Professional associations/memberships. Admitted to the Portuguese Bar Association.

David Paula, Senior Associate

Vieira de Almeida
T +351 213 113 646
F +351 213 113 406
E *dcp@vda.pt*
W *www.vda.pt*

Professional qualifications. Lawyer, Portugal

Areas of practice. Information, communication and technology in the health care, insurance, telecommunications, and financial sectors; intellectual property.

Languages. English, Spanish

Professional associations/memberships. Admitted to the Portuguese Bar Association; member of APDI (Intellectual Property Law Portuguese Association).

END OF DOCUMENT

Related Content

Topics

FinTech
Insurance
Regulatory Regime - Financial Services
Swaps and Derivatives
Security and Quasi Security