FinTech in Portugal: overview

by Tiago Correia Moreira, Helena Correia Mendonça, José Miguel Carracho and Sebastião Barros Vale, *Vieira de Almeida*

Country Q&A | Law stated as at 01-Sep-2019 | 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. This Q&A is part of the global guide to FinTech.

To compare answers across multiple jurisdictions, visit the FinTech *Country Q&A tool*. For a full list of jurisdictional Q&As visit *www.practicallaw.com/fintech-guide*.

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 the following:

- 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.
- Account information service providers.
- Crowdfunding platforms (either equity or debt-based) managing entities.

2. What are the key regulatory authorities that 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 concerning 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 more 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 significantly influenced so far?

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.

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 financing.

Payment services

The recent transposition of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) into Portuguese law (mid-November 2018) will also pave the way for new businesses (and solutions from existing ones) to enter the payment initiation services and account information services markets in 2019.

During the course of the present year, some banks in Portugal (such as *BIG* and *BPI*) have already launched services that allow their customers to access bank account information held with other credit institutions, therefore engaging in direct competition with account information service providers licenced under PSD2. Also 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 these institutions 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.

The PSD2 may enhance and further influence the FinTech ecosystem in Portugal, fostering the surge of new players and businesses along with the approach of traditional stakeholders and incumbent firms to these new innovative entities by means of business partnerships or acquisitions.

4. How do traditional financial services entities engage with FinTech?

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

It is not currently that common for cross-firm collaboration to occur between banks and solely-FinTech entities. However, with the transposition of the PSD2 into Portuguese law, the authors envisage that new partnerships in these terms will begin to arise, specifically in relation to third-party providers (TPPs) rendering services to other financial firms (for example, in relation to open banking).

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

Alternative finance

5. 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, and Law No. 3/2018 of 9 February sets out the applicable sanctions in relation to Law No. 102/2015.

This regime is also complemented by CMVM's 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 the following:

- Corporate details.
- Structure and beneficial ownership.
- Managers' identification and fit and proper documentation.
- Business plan and model.
- Indication about whether it 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.

Payment platforms

6. How is the use of FinTech in payments-related activities 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 to crowdfunding platforms.

The two current major 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, containing the Payment Services and E-Money Legal Framework (PSEMLF), which transposed PSD2 into Portuguese law.

The PSEMLF also set out the necessary regulation for payment initiation service providers (PISP) and account information service providers (AISP) to enter the Portuguese market.

The Portuguese legislator and regulatory authorities' approach to FinTech has been somewhat neutral until now, which resulted in the late transposition of the PSD2 with a delay of almost a year from the PSD2 deadline of 13 January 2018. There is also no legal approach for testing financial technology under a sandbox regime yet. This is also true from a tax perspective, where no specific Portuguese legal regime on tax incentives for FinTech exist.

However, the Portuguese financial regulators (that is, the Bank of Portugal, the Portuguese Securities Market Commission (CMVM) and the Insurance and Pension Funds Authority (ASF)) have recently implemented the Portugal FinLab programme in partnership with Portugal Fintech (a Portuguese association supporting the emerging FinTech ecosystem) 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 and concerns posed by the regulators. Additionally, the authors have also noticed an increased interest by the regulators in these matters, as the regulators have been actively participating in FinTech conferences and publishing the relevant information on their respective websites.

Investment/asset management

7. How is the use of FinTech in the securities market regulated, if at all?

The securities market is regulated under the Portuguese Securities Code, enacted by Decree-Law No. 486/99 of 13 November (as subsequently amended and currently in force) (which incorporates the changes resulting from the framework under Directive 2014/65/EU on markets in financial instruments (MiFID II)).

In terms of FinTech in the securities market, there is currently no specific regulation. 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 outside the scope of the securities laws altogether. The CMVM does not regulate cryptoassets and initial coin offerings (ICOs) unless they qualify as securities (*see Question 9*).

InsurTech

8. 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.

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

Blockchain-based solutions

9.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). However, in terms of 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.

Despite the lack of regulatory framework for blockchain itself, services resorting to smart contracts seem to have some legal comfort. Since 2007, Portugal has had a specific provision dealing with contracts automatically executed by means of computers without human intervention in its E-Commerce Law (Decree-Law No. 7/2004). This provision applies contract law to these types of contracts and further applies to programming errors, malfunctions and distorted messages the legal regime on mistake.

While self-executing or smart contracts are a step further from contracts concluded without human intervention, it seems that they are permitted under Portuguese law. Furthermore, 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.

ICOs

The BoP has (as far back as 2013) issued a clarification stating that Bitcoin (and all remaining 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 ESMA and EBA sent reports on 9 January 2019 to EU policymakers on ICOs and crypto assets assessing the applicability and suitability of EU legislation in relation to these and advising the European Commission. According to EBA's report, the competent national authorities report low crypto assets 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 crypto asset/activity.
- Specific services relating to providing crypto asset custodian wallets and crypto asset 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 crypto assets (according to the press release for ESMA's report). These gaps and issues fall into two categories:

- For crypto assets that qualify as financial instruments under MiFID, some areas require potential interpretation or re-consideration of specific requirements to allow for an effective application of existing regulations.
- For crypto assets 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 crypto assets 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 crypto assets.

ESMA therefore recommends that the European Commission either:

- Proposes a bespoke regime for specific types of crypto assets (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 ICO's 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 CMVM/ESMA is the applicable one.

Despite some lack of regulatory clarity, there seems to be some progress in acknowledging this reality, in light of the recent Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Fifth Anti-money Laundering Directive). The Fifth Anti-money Laundering Directive aims to extend the scope of application of the Fourth EU Anti-Money Laundering Directive to virtual currencies to:

- Exchange services between virtual currencies and traditional (fiat) currencies.
- Wallet providers offering custodial services of credentials necessary to hold, store and transfer virtual currencies.

Despite the amendment to the EU AML framework, the BoP clarified that financial institutions must control transfers of funds from and to platforms of negotiation of cryptocurrencies (that is, cryptocurrency exchanges) under AML legislation. In this respect, it has been widely reported that two major banks in Portugal have blocked, in the beginning of 2019, all transfers to this type of entities.

Financial services infrastructure

10. What types of financial services infrastructure-related activities of FinTech entities are regulated?

Generally, there is no specific regulation of the infrastructure and technologies underlying the FinTech sector. However, there is a set of rules and provisions addressing aspects of FinTech services with infrastructural impact, such as the following:

- The PSELF.
- 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).

Security requirements

The PSELF 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 (that is, with at least two independent authentication elements (such as password and fingerprint) mechanisms, a requirement further developed in the Regulatory Technical Standards Regulation. Payment service providers must also 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, payment service providers must also 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), Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (Electronic Identification Regulation*).
- Website authentication (*Article 3(39), Electronic Identification Regulation*).

The provision of payment services requires robust and secure infrastructures. For example, the 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 11, 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 (in 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).

Outsourcing

On 25 February 2019, EBA published its revised Guidelines for Outsourcing Arrangements (EBA/GL/2019/02). The guidelines will enter into force on 30 September 2019. The CEBS Guidelines of 2006 (GL02/2006) on outsourcing and the EBA's recommendation on outsourcing to cloud service providers will be repealed at the same time. FinTech

companies that are investment firms under MiFID II, credit institutions, payment service providers and electronic money institutions must (according to the Draft Guidelines) do the following:

- 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 which relate to critical or important functions, especially if the outsourcing concerns functions relate to core business lines and critical functions (as defined in Article 2(1)(35) and 2(1)(36) of Directive 2014/59/EU on Bank Recovery and Resolution (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) its 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 ability 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 but not limited to compliance with Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (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.

Regulatory compliance

11. What are the key regulatory compliance issues faced by FinTech entities?

FinTech companies are subject to legal regimes beyond the ones specific to the financial sector. This is the case, for instance, for data protection, cybersecurity and consumer protection. In addition, regulatory requirements for licensing, banking secrecy rules and anti-money laundering provisions also apply.

Data protection

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

These rules are those provided in Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (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 the 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, version for public consultation, adopted on 16 November 2018).

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 which 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 him/her and are based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her.

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.
- 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 impact the way FinTech companies will implement Strong Customer Authentication mechanisms under the Regulatory Technical Standards Regulation, as the Regulatory Technical Standards Regulation suggests the use of the payment service users' biometric data in that context.

Without prejudice to the above, it is important to note that the Portuguese law implementing the GDPR has entered into force (Law No. 58/2019, of 8 August). This Law 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 said financial data. In this light, the CNPD may follow the view of the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) on matters of direct marketing based on transaction data. In a letter from 3 July 2019, the Dutch authority stated clearly that all Dutch banks must review any plans of using information obtained from transactional data for direct marketing purposes as, according to the authority, such further processing for direct marketing purposes may be a violation of the purpose limitation principle established in the GDPR.

The main concern expressed by the Dutch authority is the use by banks of transactional data for direct marketing purposes without obtaining the consent from data subjects. Since the publication of the letter, Dutch banks have been suspending their direct marketing activities pending further clarifications by the authority on the matter.

Lastly, Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union (which became applicable on 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 of the European Commission's Impact Assessment Report on the Regulation). According to the 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, timeframes 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 Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems (Network and Information Security Directive) (NISD) into Portuguese law. A FinTech company may be subject to the above law's requirements 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 Regulation (EU) 575/2013 on prudential requirements for credit institutions and investment firms (Capital Requirements Regulation)) 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 providers. The NISD 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 either:
    - 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).

If FinTech companies fall under one of these definitions, they 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 the disruption of the service (in case of digital service providers); and
    - extent of the impact on economic and societal activities (in case of digital service providers).

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

Consumer protection

If FinTech companies provide services to consumers, the Consumer Law will apply. For example, information to the consumer must be provided in Portuguese.

Decree-Law 95/2006 of 29 May 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 PSELF.

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 communication to the Portuguese Consumer General Directorate (*Direção Geral do Consumidor*) is required.

Banking secrecy

Article 1 of the PSELF extends the 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 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.

In the case of processing clients' data for the purposes of anti-money laundering 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 PSELF 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 PSELF 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 EU Anti-Money Laundering Directive.

Under the Portuguese AML framework, such 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) are less stringent. These entities must only store records of the:

- Complete identification for the 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, in case of reward-based or donation-based crowdfunding.

Many compliance issues faced by FinTech relate to regulatory uncertainty in terms of the applicable laws and regulations. The amount of applicable regulation and its associated costs can be substantial (and may greatly differ depending on the type of business activity performed by the FinTech entity). If this activity requires having 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 anti-money laundering (*see above*) and KYC laws and regulations, that sometime put too much of a strain on an early-stage firm's operations. This may also be aggravated by the amount of data privacy and cybersecurity laws and regulations that may affect the FinTech entity, 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 17*).

12.Do FinTech entities encounter any additional regulatory barriers in entering into partnerships or other arrangements with traditional financial services providers? How common are these arrangements in your jurisdiction?

The authors are not aware of any existing arrangements of this sort.

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

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

Foreign entities face the same regulatory issues as domestic entities. However, 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.

14. 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, as amended).

Copyright

Copyright does not require registration to exist, but this can be done in 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 (which 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 involving 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 secret

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) have been subject to considerable revision and expansion, which is mostly related to the transposition of Directive (EU) 2016/943 on the protection of undisclosed know-how and business information against their unlawful acquisition, use and disclosure (Trade Secrets Directive). The Trade Secrets Directive substantially changed the trade secrecy regime, specifically on the protection criteria and the enforcement regime.

Government initiatives

15. To what extent have governments and/or regulators in your jurisdiction sought to create a more favourable regulatory environment for FinTech entities?

No specific measures such as regulatory sandboxes or other incentives have been created so far for FinTech firms specifically. However, there are different initiatives that are being promoted (*see Question 17*).

16. Are there any special regimes in place to facilitate access to capital for FinTech entities?

There are no special regimes to facilitate access to capital for FinTech entities. However, there are tax incentives that investors in start-ups may benefit from. 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 up to EUR100,000 in start-ups can deduct 25% of the investment made (up to a limit of 40% of the total personal income tax due).

17. Is the government taking measures to encourage foreign FinTech entities to establish a domestic presence?

No specific measures are being taken that the authors are aware of. 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 can be seen in the Startup Portugal Programme, consisting of 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

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

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

The future of FinTech

19. Are there any ongoing regulatory measures or initiatives that may affect FinTech in your jurisdiction?

The transposition of the PSD2 into Portuguese law is still very 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 even the CMVM may come

to light in the next year to address any specific issues that may occur during the market's adaptation to the new PSD2 reality, with new players emerging (notably in what concerns TPPs) and starting to interact with the established market participants.

Contributor profiles

Tiago Correia Moreira, Managing Associate

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 in 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

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

Sebastião Barros Vale, Associate

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

Professional qualifications. Lawyer, Portugal

Areas of practice. Information; communication & technology in the healthcare; insurance, telecommunications; financial sectors.

Languages. English, French, Spanish

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

END OF DOCUMENT