

IN-DEPTH

Fintech Law

PORTUGAL



LEXOLOGY

Fintech Law

EDITION 7

Contributing Editor

Thomas A Frick

Niederer Kraft Frey

In-Depth: Fintech Law (formerly The Financial Technology Law Review) provides a global overview of the fast-evolving fintech sector. It covers the most salient points of law and practice in each jurisdiction, including key licensing and other regulatory requirements, common business models and digital markets, intellectual property, data protection and much more.

Generated: April 12, 2024

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2024 Law Business Research



Explore on [Lexology](#) 

Portugal

[Tiago Correia Moreira](#), [Conceição Gamito](#), [Helena Correia Mendonça](#) and [David Paula](#)

[Vieira de Almeida & Associados](#)

Summary

[INTRODUCTION](#)

[YEAR IN REVIEW](#)

[REGULATION](#)

[DIGITAL IDENTITY AND ONBOARDING](#)

[DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING](#)

[CRYPTOCURRENCIES, INITIAL COIN OFFERINGS \(ICO\) AND SECURITY TOKENS](#)

[OTHER NEW BUSINESS MODELS](#)

[INTELLECTUAL PROPERTY AND DATA PROTECTION](#)

[OUTLOOK AND CONCLUSIONS](#)

[ENDNOTES](#)

Introduction

The regulatory treatment of fintech-related matters in Portugal greatly depends on the legal qualification of the different types of fintech companies or the products and services being offered.

The main legal and regulatory fintech concerns are those related to payment services, e-money-related activities, crowdfunding platforms and cryptoassets. The two current main categories of fintech companies are payment services institutions and e-money issuers, both of which are regulated under Decree-Law No. 91/2018 of 12 November 2018, enacting the Payment Services and E-Money Legal Framework (PSEMLF), which transposed Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 (PSD II) into the Portuguese legal framework. The PSEMLF also created the necessary regulation for third-party providers such as payment initiation service providers (PISPs) and account information service providers (AISPs) to enter the Portuguese market. Crowdfunding platforms are regulated by Law No. 102/2015 of 24 August 2015 and Law No. 3/2018 of 9 February 2018, as well as by the Portuguese Securities Market Commission (CMVM) Regulation 1/2016. More recently, some traditional market players have also been positioning themselves in the fintech-related segment, either because they have developed state-of-the-art technology to pursue intermediation activities or because they have partnered with startups and scale-ups in offering user-friendly banking solutions.

Since 1 September 2020, the Bank of Portugal (BoP) has been the competent authority for registering and verifying compliance with the applicable legal and regulatory provisions governing anti-money laundering and countering the financing of terrorism (AML/CFT) by the entities that carry out certain activities involving virtual assets. However, it should be clarified that the BoP's responsibility is limited to AML/CFT prevention and does not cover other domains of prudential banking conduct.

The Portuguese legislator and regulatory authorities' approach to fintech had been somewhat neutral, which resulted in the late transposition of PSD II (a delay of almost a year from the 13 January 2018 deadline). This is also true from a tax perspective, as no specific legal regime exists in Portugal for fintech-related tax incentives.

In 2021, the Portuguese government approved Decree-Law No. 67/2021 of 30 July 2021, which establishes the legal framework and defines the governance model for the promotion of tech-based innovation through the creation of technological free zones (ZLTs). This Law does not create ZLTs per se but establishes the basic conditions for their future creation by interested parties (each of which will require a separate act). While ZLTs are, in fact and in accordance with this Law, considered regulatory sandboxes, because the proper regulatory authorities will directly and permanently monitor tests carried out in them, the aim is to go beyond the creation of disparate 'regulatory sandboxes', 'innovation spaces', 'experimental spaces' or 'living labs' that are set up for specific sectors and instead to adopt a cross-sector and integrated approach (i.e., that crosses more than one sector and may therefore be subject to different regulations and regulators, including the BoP and the CMVM) for experimentation activities, therefore reducing burdens and promoting a culture of experimentation. The first ZLT was implemented in Portugal during the year 2022.

In addition to the above, the Portuguese financial regulators (i.e., the BoP, the CMVM and the Insurance and Pension Funds Authority) implemented the Portugal FinLab programme (now in its fifth edition) with the purpose of establishing an easily accessible communication channel between entrepreneurs and emerging companies, on the one hand, and the financial regulators, on the other, aimed at supporting fintech businesses and companies in navigating the legal and regulatory challenges and concerns posed by the regulators. Additionally, regulators have shown increased interest in these matters, as demonstrated by their participation in fintech-related conferences and the disclosure on their websites of information released during these conferences.

The regulatory treatment of fintech-related matters in Portugal greatly depends on the legal qualification of the different types of fintech companies or the products and services being offered.

The main legal and regulatory fintech concerns are those related to payment services, e-money-related activities, crowdfunding platforms and cryptoassets. The two current main categories of fintech companies are payment services institutions and e-money issuers, both of which are regulated under Decree-Law No. 91/2018 of 12 November 2018, enacting the Payment Services and E-Money Legal Framework (PSEMLF), which transposed Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 (PSD II) into the Portuguese legal framework. The PSEMLF also created the necessary regulation for third-party providers such as payment initiation service providers (PISPs) and account information service providers (AISPs) to enter the Portuguese market. Crowdfunding platforms are regulated by Law No. 102/2015 of 24 August 2015 and Law No. 3/2018 of 9 February 2018, as well as by the Portuguese Securities Market Commission (CMVM) Regulation 1/2016. More recently, some traditional market players have also been positioning themselves in the fintech-related segment, either because they have developed state-of-the-art technology to pursue intermediation activities or because they have partnered with startups and scale-ups in offering user-friendly banking solutions.

Since 1 September 2020, the Bank of Portugal (BoP) has been the competent authority for registering and verifying compliance with the applicable legal and regulatory provisions governing anti-money laundering and countering the financing of terrorism (AML/CFT) by the entities that carry out certain activities involving virtual assets. However, it should be clarified that the BoP's responsibility is limited to AML/CFT prevention and does not cover other domains of prudential banking conduct.

The Portuguese legislator and regulatory authorities' approach to fintech had been somewhat neutral, which resulted in the late transposition of PSD II (a delay of almost a year from the 13 January 2018 deadline). This is also true from a tax perspective, as no specific legal regime exists in Portugal for fintech-related tax incentives.

In 2021, the Portuguese government approved Decree-Law No. 67/2021 of 30 July 2021, which establishes the legal framework and defines the governance model for the promotion of tech-based innovation through the creation of technological free zones (ZLTs). This Law does not create ZLTs per se but establishes the basic conditions for their future creation by interested parties (each of which will require a separate act). While ZLTs are, in fact and in accordance with this Law, considered regulatory sandboxes, because the proper regulatory authorities will directly and permanently monitor tests carried out in them, the aim is to go beyond the creation of disparate 'regulatory sandboxes', 'innovation spaces', 'experimental spaces' or 'living labs' that are set up for specific sectors and instead to

adopt a cross-sector and integrated approach (i.e., that crosses more than one sector and may therefore be subject to different regulations and regulators, including the BoP and the CMVM) for experimentation activities, therefore reducing burdens and promoting a culture of experimentation. The first ZLT was implemented in Portugal during the year 2022.

In addition to the above, the Portuguese financial regulators (i.e., the BoP, the CMVM and the Insurance and Pension Funds Authority) implemented the Portugal FinLab programme (now in its fifth edition) with the purpose of establishing an easily accessible communication channel between entrepreneurs and emerging companies, on the one hand, and the financial regulators, on the other, aimed at supporting fintech businesses and companies in navigating the legal and regulatory challenges and concerns posed by the regulators. Additionally, regulators have shown increased interest in these matters, as demonstrated by their participation in fintech-related conferences and the disclosure on their websites of information released during these conferences.

Year in review

There has been no material change to fintech-specific regulation during the past 18 months, and while new players might have been expected to appear in the short to medium term, that does not seem to have been the case, except for the cross-border crowdfunding platforms.

Additionally, the BoP's new registration regime in respect of certain entities that pursue activities involving virtual assets may attract entities operating in these core areas, and new players may appear through this route.

Portugal Fintech, a Portuguese association supporting the emerging fintech ecosystem, continues its mission to promote the Portuguese fintech market, by gathering fintech, regtech, insurtech and cybersecurity companies in Portugal and fostering their access to and visibility among legislators, startups, investors, consultants, banks, regulators and other relevant entities.

The Portugal FinLab, an acceleration programme providing a communication channel between new market players (or even established institutions with innovative tech-based financial projects or products) and the Portuguese regulatory authorities, is now in its third edition. Through this programme, the regulators provide guidance and support to participants, without the usual hurdles, on how to navigate and operate in the existing regulatory system.

The Portuguese legal framework on ZLTs was approved in 2021, setting up the main principles and rules for the creation of ZLTs – regulatory sandboxes crossing more than one sector and that may be subject to different regulations and regulators (such as the BoP and the CMVM). ZLTs aim to facilitate testing and experimentation activities of new technologies, products, services and processes, therefore reducing burdens and promoting a culture of innovation in the country. The first ZLT was implemented in Portugal during the year 2022.

There has been no material change to fintech-specific regulation during the past 18 months, and while new players might have been expected to appear in the short to medium

term, that does not seem to have been the case, except for the cross-border crowdfunding platforms.

Additionally, the BoP's new registration regime in respect of certain entities that pursue activities involving virtual assets may attract entities operating in these core areas, and new players may appear through this route.

Portugal Fintech, a Portuguese association supporting the emerging fintech ecosystem, continues its mission to promote the Portuguese fintech market, by gathering fintech, regtech, insurtech and cybersecurity companies in Portugal and fostering their access to and visibility among legislators, startups, investors, consultants, banks, regulators and other relevant entities.

The Portugal FinLab, an acceleration programme providing a communication channel between new market players (or even established institutions with innovative tech-based financial projects or products) and the Portuguese regulatory authorities, is now in its third edition. Through this programme, the regulators provide guidance and support to participants, without the usual hurdles, on how to navigate and operate in the existing regulatory system.

The Portuguese legal framework on ZLTs was approved in 2021, setting up the main principles and rules for the creation of ZLTs – regulatory sandboxes crossing more than one sector and that may be subject to different regulations and regulators (such as the BoP and the CMVM). ZLTs aim to facilitate testing and experimentation activities of new technologies, products, services and processes, therefore reducing burdens and promoting a culture of innovation in the country. The first ZLT was implemented in Portugal during the year 2022.

Regulation

i Licensing and marketing

The PSEMLF sets out the applicable rules and requirements for the incorporation and licensing of payment institutions and e-money issuers as well as PISPs and AISPs, all being subject to the BoP's supervision. To that effect, specific mandatory legal documentation must be filed with the BoP, including draft by-laws, business plan, share capital commitment, corporate structure and beneficial ownership, the managers' identification and fit and proper documentation, as well as corporate governance and internal compliance models and procedures. The minimum statutory share capital requirement currently applicable to payment institutions ranges from a minimum of €20,000 to €125,000 (depending on the type of services provided) and a minimum of €350,000 for e-money institutions. PISPs must have a minimum statutory share capital of €50,000, and AISPs are required to acquire an insurance policy or other similar guarantee scheme covering their activity in the Portuguese territory in the case of a breach or unauthorised access to data.

All marketing and advertising carried out by these entities must abide by the general rules applicable to marketing and advertising by banks and other financial institutions. This means that, among other requirements, all marketing and advertisement products and

materials must clearly identify the offering or advertising entity, while also ensuring that the main features and conditions of the marketed products or services are easily understood by targeted consumers.

The PSEMLF provides for an extensive list of products and services that may only be offered by payment or e-money institutions, as well as PISPs or AISPs. This means that, in practice, considering the nature and business model of most fintech companies and the services offered, they will have to qualify as one of these entities under Portuguese law (as an entity with an e-money licence ensures that it can render all services regulated under the PSEMLF, provided that it requests an authorisation to that effect when registering with the BoP), thus having to comply with its regulatory framework.

In what concerns crowdfunding platforms, Portuguese law sets out requirements and conditions applicable to the corporate entities managing these platforms, which are subject to the CMVM's supervision when they are either collaborative equity-based or loan-based platforms. These management entities of crowdfunding platforms are subject to prior registry and authorisation with the CMVM. Their application must be accompanied by the required documentation, which includes the entity's corporate details, structure and beneficial ownership, the managers' identification and fit and proper documentation, business plan and model, and an indication of whether it should be considered a financial intermediary or an agent thereof, as well as evidence of compliance with the minimum financial requirements. Currently there are already more than 20 crowdfunding platforms registered with the CMVM that are authorised to provide such services in Portugal.

In addition, entities that carry out any of the following activities involving virtual assets must be registered with the BoP for the purposes of verifying compliance with the applicable legal and regulatory provisions governing AML/CFT:

1. exchange services between virtual assets and fiat money or between one or more virtual assets;
2. virtual asset transfer services; and
3. services of safekeeping, or safekeeping and administration of virtual assets or of instruments that enable the control, ownership, storage or transfer of these assets, including private encrypted keys.

Currently, there are 12 entities registered with the BoP in this respect, though five out of those 12 have not initiated their activities.

ii Cross-border issues

Payment or e-money institutions based abroad may render their services in Portugal, subject to prior authorisation and registry with the BoP. The applicable requirements and procedures may vary according to the state of origin, as entities based in EU Member States can choose to render their services in Portugal through a branch registered in Portugal, through authorised agents based in Portugal (notably in what concerns e-money distribution) or under a licence granting them the freedom to provide services.

Should the applying entity be based in a third-country state, it shall incorporate a branch or, alternatively, incorporate a subsidiary legal entity in the Portuguese territory (by following the relevant, though more demanding, procedure).

Digital identity and onboarding

Portuguese citizens must have a citizenship card containing their relevant identification data, which includes a civil identification number, taxpayer number, healthcare user number and social security number (Law No. 7/2007 creating the citizenship card, as amended). The citizenship card proves the identity of its holder to any public or private authorities and entities, through two mechanisms:

1. by the reading of the visible elements of the card, together with the optical reading of a reserved area of the card (this optical reading is mainly limited to state or public administration entities or services); and
2. by means of electronic authentication.

The citizenship card further allows its holder to unambiguously authenticate authorship of electronic documents by means of an electronic signature. The card contains a chip where additional information is available, such as address and fingerprints – it is in this chip that the certificates for secure authentication and for the qualified electronic signature are available. Hence, the holder of a Portuguese citizenship card has two digital certificates: one for authentication and another for e-signature. The security and technology features of the citizen cards produced in the course of 2023 will also be improved to permit its contactless use.

Law No. 7/2007 expressly refers to Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions (the eIDAS Regulation), indicating that the provisions established therein apply to the certificates. However, when it comes to electronic identification and trust services, including e-signatures, electronic seals and time stamps, Decree-Law No. 12/2021 is the legislation that consolidates the Portuguese rules on electronic identification, including the probative value of e-signatures. There is a proposal for a Regulation amending the eIDAS Regulation under which EU Member States shall provide EU digital identity wallets free of charge, which can be used, for instance, as electronic national ID cards, electronic passports or identification for online services or for signing digital agreements.

Furthermore, Law No. 37/2014, as amended, created the 'digital mobile key', which is an additional and voluntary means of:

1. authenticating electronic systems and internet sites; and
2. providing a qualifying e-signature in the terms indicated in the eIDAS Regulation.

All citizens may request to associate their civil identification number with a mobile phone number or an email address. Foreign citizens without a civil identification number may also request this association, which is carried out through their passport number, their tax identification on residence permits (or other documents, as indicated in the regime for the

entry, stay, exit and expulsion of foreigners from national territory) or their residence card. The digital mobile key is a secure authentication system comprising a permanent password and a numerical code issued for each use and generated by the system. Decree-Law No. 88/2021 of 3 November 2021 last amended Law No. 37/2014, noting the increasing use of the digital mobile key across several sectors (including in the banking sector), and the need to further develop mechanisms for accessing online digital services as a result of the covid-19 pandemic. This Act, among other points, simplified the authentication process with the digital mobile key through mobile application and biometrics.

Financial service providers, including payment institutions and e-money institutions, may carry out fully digitised onboarding of clients, including, as of recently, by using videoconferencing procedures.

BoP Notice No. 12/2022 allows financial institutions to make use of remote onboarding procedures while complying with the know-your-customer (KYC) requirements set out under the applicable AML framework. At present, the admissible remote onboarding procedures under applicable AML law and Notice No. 1/2022 are videoconferencing and other means of KYC and onboarding procedures carried out by qualified trust service providers (the latter being compliant with the framework set forth under Regulation (EU) 910/2014).

On 22 November 2022, the European Banking Authority (EBA) also published its Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15) aimed at providing guidance to financial institutions and regulators on how to use remote customer onboarding solutions in a way that is secure, transparent and compliant with applicable laws and regulations, including the applicable AML/CFT legislation and the EU's data protection framework.

Portuguese citizens must have a citizenship card containing their relevant identification data, which includes a civil identification number, taxpayer number, healthcare user number and social security number (Law No. 7/2007 creating the citizenship card, as amended). The citizenship card proves the identity of its holder to any public or private authorities and entities, through two mechanisms:

1. by the reading of the visible elements of the card, together with the optical reading of a reserved area of the card (this optical reading is mainly limited to state or public administration entities or services); and
2. by means of electronic authentication.

The citizenship card further allows its holder to unambiguously authenticate authorship of electronic documents by means of an electronic signature. The card contains a chip where additional information is available, such as address and fingerprints – it is in this chip that the certificates for secure authentication and for the qualified electronic signature are available. Hence, the holder of a Portuguese citizenship card has two digital certificates: one for authentication and another for e-signature. The security and technology features of the citizen cards produced in the course of 2023 will also be improved to permit its contactless use.

Law No. 7/2007 expressly refers to Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions (the eIDAS Regulation), indicating that

the provisions established therein apply to the certificates. However, when it comes to electronic identification and trust services, including e-signatures, electronic seals and time stamps, Decree-Law No. 12/2021 is the legislation that consolidates the Portuguese rules on electronic identification, including the probative value of e-signatures. There is a proposal for a Regulation amending the eIDAS Regulation under which EU Member States shall provide EU digital identity wallets free of charge, which can be used, for instance, as electronic national ID cards, electronic passports or identification for online services or for signing digital agreements.

Furthermore, Law No. 37/2014, as amended, created the 'digital mobile key', which is an additional and voluntary means of:

1. authenticating electronic systems and internet sites; and
2. providing a qualifying e-signature in the terms indicated in the eIDAS Regulation.

All citizens may request to associate their civil identification number with a mobile phone number or an email address. Foreign citizens without a civil identification number may also request this association, which is carried out through their passport number, their tax identification on residence permits (or other documents, as indicated in the regime for the entry, stay, exit and expulsion of foreigners from national territory) or their residence card. The digital mobile key is a secure authentication system comprising a permanent password and a numerical code issued for each use and generated by the system. Decree-Law No. 88/2021 of 3 November 2021 last amended Law No. 37/2014, noting the increasing use of the digital mobile key across several sectors (including in the banking sector), and the need to further develop mechanisms for accessing online digital services as a result of the covid-19 pandemic. This Act, among other points, simplified the authentication process with the digital mobile key through mobile application and biometrics.

Financial service providers, including payment institutions and e-money institutions, may carry out fully digitised onboarding of clients, including, as of recently, by using videoconferencing procedures.

BoP Notice No. 12/2022 allows financial institutions to make use of remote onboarding procedures while complying with the know-your-customer (KYC) requirements set out under the applicable AML framework. At present, the admissible remote onboarding procedures under applicable AML law and Notice No. 1/2022 are videoconferencing and other means of KYC and onboarding procedures carried out by qualified trust service providers (the latter being compliant with the framework set forth under Regulation (EU) 910/2014).

On 22 November 2022, the European Banking Authority (EBA) also published its Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15) aimed at providing guidance to financial institutions and regulators on how to use remote customer onboarding solutions in a way that is secure, transparent and compliant with applicable laws and regulations, including the applicable AML/CFT legislation and the EU's data protection framework.

Digital markets, payment services and funding

Both payment and e-money institutions, as well as PISPs and AISPs and the management entities of crowdfunding platforms, are subject to licensing and registry requirements with either the BoP or the CMVM, respectively. A new regime has also been created for certain entities that pursue activities involving virtual assets to be registered with the BoP.

Crowdfunding schemes are gaining some traction as mentioned above. Most of the developments arise following the entry into force of the Regulation on European Crowdfunding Service Providers for Business, and as the market develops and market players become more sophisticated and numerous.

In June 2019, Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services came into force, placing certain obligations upon providers of online intermediation services, simultaneously:

1. constituting information society services;^[2]
2. allowing business users to offer goods or services to consumers; and
3. providing to business users based on contractual relationships (such as platforms' terms of use).

Obligations include transparency and intelligibility requirements for platforms' terms and conditions, duties of notification to business users concerning changes to those terms and conditions, limitations on the restriction, suspension and termination of online intermediation services, explanation of ranking parameters (when the online intermediation services include these rankings), transparency with respect to the differentiated treatment of business users and the service provider's access to personal data through the platform, and the setting up of an internal complaint-handling system with specific characteristics (without prejudice against the possibility of business users resorting to mediation).

The Digital Markets Act (DMA), designed to address the growing power of digital platforms and the need to create a more level playing field and promote fair competition in the digital sector should also have significant relevance for fintech companies operating within the European Union. In fact, one of the key provisions of the DMA is the creation of a new regulatory framework for 'gatekeeper' platforms, which are defined as large online platforms that have significant market power and act as intermediaries between businesses and consumers. Fintech companies operating within the digital sector may be affected by the DMA if they use gatekeeper platforms to reach customers or if they themselves are considered gatekeepers.

Both payment and e-money institutions, as well as PISPs and AISPs and the management entities of crowdfunding platforms, are subject to licensing and registry requirements with either the BoP or the CMVM, respectively. A new regime has also been created for certain entities that pursue activities involving virtual assets to be registered with the BoP.

Crowdfunding schemes are gaining some traction as mentioned above. Most of the developments arise following the entry into force of the Regulation on European Crowdfunding Service Providers for Business, and as the market develops and market players become more sophisticated and numerous.

In June 2019, Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services came into force, placing certain obligations upon providers of online intermediation services, simultaneously:

1. constituting information society services;^[2]
2. allowing business users to offer goods or services to consumers; and
3. providing to business users based on contractual relationships (such as platforms' terms of use).

Obligations include transparency and intelligibility requirements for platforms' terms and conditions, duties of notification to business users concerning changes to those terms and conditions, limitations on the restriction, suspension and termination of online intermediation services, explanation of ranking parameters (when the online intermediation services include these rankings), transparency with respect to the differentiated treatment of business users and the service provider's access to personal data through the platform, and the setting up of an internal complaint-handling system with specific characteristics (without prejudice against the possibility of business users resorting to mediation).

The Digital Markets Act (DMA), designed to address the growing power of digital platforms and the need to create a more level playing field and promote fair competition in the digital sector should also have significant relevance for fintech companies operating within the European Union. In fact, one of the key provisions of the DMA is the creation of a new regulatory framework for 'gatekeeper' platforms, which are defined as large online platforms that have significant market power and act as intermediaries between businesses and consumers. Fintech companies operating within the digital sector may be affected by the DMA if they use gatekeeper platforms to reach customers or if they themselves are considered gatekeepers.

Cryptocurrencies, initial coin offerings (ICO) and security tokens

Blockchain or distributed ledger technology is not subject to specific regulation in Portugal as a technology. The regulation brought by blockchain has been essentially focused on the banking and finance sector, including cryptocurrencies and ICOs, notably in what concerns investor protection and fraud prevention. There is currently no regulation on the tokenisation of assets in general (and securities in particular, such as bonds or shares), although nothing in the law seems to generally prohibit it. As such, in principle we see no impediment to the tokenisation of assets or credits, provided that the parties involved in a given transaction agree on the dematerialisation of the agreement or title and the underlying assets (and the corresponding representation of the assets by tokens). Notwithstanding the above, in principle it would not be applicable to those assets subject to special registration or notarisation formalities (such as real estate assets) as this would additionally entail formal legal recognition by the governmental or registration authorities.

However, in Portugal the approach in this sector has been to generally exclude cryptocurrencies from being qualified as tender or 'legal currency' and not to issue specific regulations dealing with them. As far back as 2013,^[3] the BoP issued a clarification under which it considered that Bitcoin cannot be considered secure currency, given that its issuing is carried out by non-regulated and non-supervised entities. In addition, the BoP clarified this and stated that users bear all the risk, as there is no fund or protection scheme guaranteeing depositors' or investors' funds. This approach closely follows the position of the EBA. Despite the lack of regulation and supervision, the BoP has indicated that the use of cryptocurrencies is not a forbidden or illegal act. Hence, this entity is so far more focused on a preventive and educational approach, by means of alerting to the risks of cryptocurrencies.

Both the BoP and the CMVM share this understanding and – like the majority of European regulators – have been pursuing a wait-and-see approach towards regulation at the European level, which has culminated in the proposal for regulations contained in the Digital Finance Package (notably the Regulation on Markets in Crypto-assets (MiCA)), which will bring a broader and harmonised European framework applicable to both cryptoassets and blockchain technology.

Until these regulations are effectively enacted and come into force, a different case-by-case approach should be taken regarding those assets qualifying as securities, such as security tokens or other hybrid tokens comprising some security-like traits, pursuant to the European Securities and Markets Authority (ESMA) advice dated 9 January 2019,^[4] whereas cryptoassets qualifying as transferable securities (or another type of financial instrument under the Markets in Financial Instruments Directive (MiFID) II criteria) should be subject to the broader EU financial rules in this respect (including MiFID II and the Prospectus and Market Abuse Directives). Although the definition of what qualifies as a 'security' has been mostly committed to national regulation implementing EU legislation, we would expect to see the CMVM adopt the same approach as ESMA and to decide on the applicability of the legal framework applicable to securities (including that of public offerings, in the case of ICOs) on a case-by-case basis. An example of this approach was seen in 2018 in the context of the Bityond ICO, where the CMVM decided not to apply the public offerings regime (and the securities legal framework as a whole) after having analysed the white paper and the token's configuration and associated rights and obligations, which did not present traits similar to those of tradeable securities.

ESMA has identified a number of concerns regarding the current financial regulatory framework as applies to cryptoassets. These concerns and 'gaps' fall under two categories:

1. for cryptoassets that qualify as financial instruments under MiFID, there are areas that potentially require interpretation or reconsideration of specific requirements to allow for an effective application of existing securities and financial regulations; and
2. where these assets do not qualify as financial instruments, the absence of applicable financial rules leaves investors exposed to substantial risks. At a minimum, ESMA believes that AML requirements should apply to all cryptoassets and activities involving cryptoassets. There should also be appropriate risk disclosure in place, so that consumers can be made aware of the potential risks prior to committing funds to cryptoassets.

Considering the above, the usual distinction between different types of tokens (or rather, the rights and obligations that their issuance and possession entail) underlying the transactions may prove useful. Where tokens are used mainly as a means of payment, the approach taken by the BoP and the EBA is the one to look at. Conversely, where tokens share more similarities with securities, the approach taken by the CMVM and ESMA is the one to note.

Despite a slight lack of regulatory clarity, some progress appears to have been made in acknowledging this situation, considering the approved version of the MiCA regulation and the pilot regime for market infrastructures based on distributed ledger technology, under the Digital Finance Package, which is expected to see further material developments in the near future.

Law No. 58/2020 of 31 August 2020 transposed the recent AML Directive changes, extending its scope of application to virtual currencies (namely, to crypto exchanges and wallet providers offering custodial services) and imposing an obligation to register with the BoP and to comply with KYC and AML procedures with respect to their clients and the transactions taking place in their exchanges or wallets.

The year 2023 marked a turning point in the Portuguese tax framework for cryptocurrencies and other cryptoassets. This came about with the approval of specific tax rules that became effective on 1 January 2023.

This tax framework was implemented at a moment when, on the European scene, we saw, on the one hand, a Regulation establishing a European framework for cryptoasset markets (MiCA Regulation) approved by the European Council^[5] and, on the other hand, complementing this Regulation, new tax transparency rules approved^[6] for all service providers facilitating transactions in cryptoassets for customers resident in the European Union. Also setting the agenda for this year and the coming years is the VAT in the Digital Age (ViDA) package. The ViDA package is divided in three pillars: (1) Digital Reporting Requirements and e-invoicing; (2) the VAT treatment of the platform economy; and (3) a single place of VAT registration. ViDA translates into three proposals amending the VAT Directive^[7], the VAT Implementing Regulation^[8] and the Regulation (EU) No. 904/2010 on administrative cooperation. In a nutshell, the Portuguese cryptoasset tax framework can be divided into the following four main blocks.

Blockchain or distributed ledger technology is not subject to specific regulation in Portugal as a technology. The regulation brought by blockchain has been essentially focused on the banking and finance sector, including cryptocurrencies and ICOs, notably in what concerns investor protection and fraud prevention. There is currently no regulation on the tokenisation of assets in general (and securities in particular, such as bonds or shares), although nothing in the law seems to generally prohibit it. As such, in principle we see no impediment to the tokenisation of assets or credits, provided that the parties involved in a given transaction agree on the dematerialisation of the agreement or title and the underlying assets (and the corresponding representation of the assets by tokens). Notwithstanding the above, in principle it would not be applicable to those assets subject to special registration or notarisation formalities (such as real estate assets) as this would additionally entail formal legal recognition by the governmental or registration authorities.

However, in Portugal the approach in this sector has been to generally exclude cryptocurrencies from being qualified as tender or 'legal currency' and not to issue specific regulations dealing with them. As far back as 2013,^[3] the BoP issued a clarification under

which it considered that Bitcoin cannot be considered secure currency, given that its issuing is carried out by non-regulated and non-supervised entities. In addition, the BoP clarified this and stated that users bear all the risk, as there is no fund or protection scheme guaranteeing depositors' or investors' funds. This approach closely follows the position of the EBA. Despite the lack of regulation and supervision, the BoP has indicated that the use of cryptocurrencies is not a forbidden or illegal act. Hence, this entity is so far more focused on a preventive and educational approach, by means of alerting to the risks of cryptocurrencies.

Both the BoP and the CMVM share this understanding and – like the majority of European regulators – have been pursuing a wait-and-see approach towards regulation at the European level, which has culminated in the proposal for regulations contained in the Digital Finance Package (notably the Regulation on Markets in Crypto-assets (MiCA)), which will bring a broader and harmonised European framework applicable to both cryptoassets and blockchain technology.

Until these regulations are effectively enacted and come into force, a different case-by-case approach should be taken regarding those assets qualifying as securities, such as security tokens or other hybrid tokens comprising some security-like traits, pursuant to the European Securities and Markets Authority (ESMA) advice dated 9 January 2019,¹ ⁴⁾ whereas cryptoassets qualifying as transferable securities (or another type of financial instrument under the Markets in Financial Instruments Directive (MiFID) II criteria) should be subject to the broader EU financial rules in this respect (including MiFID II and the Prospectus and Market Abuse Directives). Although the definition of what qualifies as a 'security' has been mostly committed to national regulation implementing EU legislation, we would expect to see the CMVM adopt the same approach as ESMA and to decide on the applicability of the legal framework applicable to securities (including that of public offerings, in the case of ICOs) on a case-by-case basis. An example of this approach was seen in 2018 in the context of the Bityond ICO, where the CMVM decided not to apply the public offerings regime (and the securities legal framework as a whole) after having analysed the white paper and the token's configuration and associated rights and obligations, which did not present traits similar to those of tradeable securities.

ESMA has identified a number of concerns regarding the current financial regulatory framework as applies to cryptoassets. These concerns and 'gaps' fall under two categories:

1. for cryptoassets that qualify as financial instruments under MiFID, there are areas that potentially require interpretation or reconsideration of specific requirements to allow for an effective application of existing securities and financial regulations; and
2. where these assets do not qualify as financial instruments, the absence of applicable financial rules leaves investors exposed to substantial risks. At a minimum, ESMA believes that AML requirements should apply to all cryptoassets and activities involving cryptoassets. There should also be appropriate risk disclosure in place, so that consumers can be made aware of the potential risks prior to committing funds to cryptoassets.

Considering the above, the usual distinction between different types of tokens (or rather, the rights and obligations that their issuance and possession entail) underlying the transactions may prove useful. Where tokens are used mainly as a means of payment, the approach

taken by the BoP and the EBA is the one to look at. Conversely, where tokens share more similarities with securities, the approach taken by the CMVM and ESMA is the one to note.

Despite a slight lack of regulatory clarity, some progress appears to have been made in acknowledging this situation, considering the approved version of the MiCA regulation and the pilot regime for market infrastructures based on distributed ledger technology, under the Digital Finance Package, which is expected to see further material developments in the near future.

Law No. 58/2020 of 31 August 2020 transposed the recent AML Directive changes, extending its scope of application to virtual currencies (namely, to crypto exchanges and wallet providers offering custodial services) and imposing an obligation to register with the BoP and to comply with KYC and AML procedures with respect to their clients and the transactions taking place in their exchanges or wallets.

The year 2023 marked a turning point in the Portuguese tax framework for cryptocurrencies and other cryptoassets. This came about with the approval of specific tax rules that became effective on 1 January 2023.

This tax framework was implemented at a moment when, on the European scene, we saw, on the one hand, a Regulation establishing a European framework for cryptoasset markets (MiCA Regulation) approved by the European Council^[5] and, on the other hand, complementing this Regulation, new tax transparency rules approved^[6] for all service providers facilitating transactions in cryptoassets for customers resident in the European Union. Also setting the agenda for this year and the coming years is the VAT in the Digital Age (ViDA) package. The ViDA package is divided in three pillars: (1) Digital Reporting Requirements and e-invoicing; (2) the VAT treatment of the platform economy; and (3) a single place of VAT registration. ViDA translates into three proposals amending the VAT Directive^[7], the VAT Implementing Regulation^[8] and the Regulation (EU) No. 904/2010 on administrative cooperation. In a nutshell, the Portuguese cryptoasset tax framework can be divided into the following four main blocks.

i First block

The first block establishes a legal definition of cryptoassets for tax purposes. A comprehensive cryptoasset definition for tax purposes is provided in the law as 'any digital representation of value or rights that can be transferred or stored electronically using distributed recording or similar technology'. This definition is, in fact, very broad and is intended to cover most types of cryptoassets, such as cryptocurrencies, stablecoins, utility tokens and security tokens, but expressly excludes 'unique crypto-assets that are not fungible with other crypto-assets' (i.e., non-fungible tokens – NFTs).

ii Second block

The second block deals with the taxation of income from transactions with cryptoassets. We highlight that, for personal income tax (PIT) purposes, income that is derived from the issuance of cryptoassets (e.g., through mining activities) or from the validation of transactions with cryptoassets through consensus mechanisms and capital gains derived from the disposal of cryptoassets, within the scope of a business or professional activity, will be taxed as business or professional income (i.e., under PIT 'Category B' income).

For the determination of the taxable income derived from these activities by taxpayers covered by the PIT simplified regime,^[9] a 0.95 coefficient is applied to the income derived from mining activities and a 0.15 coefficient to business or professional income derived from other transactions with cryptoassets. The deduction of expenses is not allowed under the PIT simplified regime. For taxpayers covered by the PIT organised accounting regime,^[10] the taxable income will consist of the amount of income obtained. Under the organised accounting regime, the deduction of expenses actually incurred and essential to obtaining that income is allowed. The relevant taxable income, whether calculated under the simplified regime or the organised accounting regime rules described above, will be taxed at the PIT progressive rates, with the possible application of solidarity surcharges.^[11]

Gains from the disposal for consideration of cryptoassets, derived outside the scope of a business or professional activity, are not taxed under Category B, but are instead qualified as capital gains, taxable under PIT 'Category G' income. However, while capital gains on cryptoassets that do not qualify as securities and are held for less than one year, are taxed at a flat rate of 28 per cent (this rate does not apply in the event the taxpayer opts for the income aggregation; in such case, PIT progressive rates will apply, as well as possible solidarity surcharges, and taxpayers may carry forward negative balance for up to five years), capital gains on cryptoassets that do not qualify as securities^[12] and are held for more than 365 days are excluded from taxation. Capital gains on cryptoassets that qualify as securities are taxed at a flat rate of 28 per cent. This rate does not apply in the event the taxpayer opts for the income aggregation. In such case, PIT progressive rates will apply, as well as possible solidarity surcharges, and taxpayers may carry forward a negative balance for up to five years. However, if the cryptoassets qualify as securities and are held for less than one year, and the taxpayer has a taxable income equal to or greater than the highest bracket,^[13] aggregation is mandatory. Where the consideration for the disposal of the cryptoassets takes the form of other cryptoassets, cryptoassets received will be attributed the acquisition value of the cryptoassets delivered, thus deferring taxation to the moment when the capital gain is actually realised. The relevant disposal value for a cryptoasset is considered to be its market value at the date of disposal. The relevant capital gain for PIT purposes is the difference between the realisation value and the acquisition value, net of the part qualified as capital income, if any, and the deduction of expenses necessary and actually incurred to the acquisition of the cryptoassets is allowed. The FIFO (First In First Out) rule is applied to cryptoassets, considering for the purposes of calculating the balance of capital gains that those that were acquired more recently are sold. In the event that the option for aggregation is exercised (as opposed to the taxation at a flat rate of 28 per cent), capital losses may be carried forward for the following five years.

Nevertheless, for PIT purposes, any form of remuneration derived from transactions with cryptoassets (e.g., staking) that are not qualified as business or professional income will qualify as investment income, taxable under PIT 'Category E' income. This income is subject to a tax rate of 28 per cent and, irrespective of the form it takes (i.e., even when paid in cash), it is exempt from withholding tax. However, when the consideration takes the form of other cryptoassets, this income will be taxed under PIT 'Category G' income as capital gains, but only at the moment of disposal of the cryptoassets received.

For anti-avoidance purposes, it is provided that neither the deferral of taxation when the consideration takes the form of other cryptoassets, nor the exclusion from taxation for cryptoassets that do not qualify as securities and are held for more than 365 days, will apply

to a person or entity that is not a tax resident in another Member State of the European Union or the European Economic Area or in another state or jurisdiction with which a double tax treaty or a bilateral or multilateral agreement bilateral or multilateral agreement that provides for the exchange of information for tax purposes is in force. Furthermore, cryptoassets are deemed to have been disposed of in the event of termination of activity or of loss of the status of resident in the Portuguese territory. In the event of loss of resident status, it is also provided that the relevant taxable income is determined by the positive difference between the market value at the date the resident status is lost and the acquisition value, plus the expenses necessary and actually incurred to the acquisition of the cryptoassets.

For corporate income tax (CIT) purposes, income derived from the issuance of cryptoassets (e.g., through mining activities) or from the validation of transactions with cryptoassets through consensus mechanisms is considered as income derived from commercial or industrial activities and is subject to CIT. Similarly, to the PIT rules, under the simplified regime^[14] a coefficient of 0.15 should be applied for the determination of the taxable income arising from these activities. Thus, in practice, only 15 per cent of the taxable income derived from these activities will be subject to taxation.

Also, noteworthy is the reporting obligation that applies to any person or entity, with or without legal personality, providing cryptoasset custody and management services on behalf of third parties or managing one or more cryptoasset trading platforms. All of those covered by this reporting obligation will have to report to the Portuguese Tax Authority all cryptoasset transactions carried out with their intervention.

iii Third block

The third block is focused on taxation on wealth transfer, covering certain transfers of cryptoassets. For cryptoassets deposited in institutions having their head office, effective management or permanent establishment in Portuguese territory (as well as in the case of non-deposited cryptoassets, in the case of succession due to death, when the transferor is domiciled in Portuguese territory or in other gratuitous transfers), when the beneficiary is domiciled in Portuguese territory, the new rules provide that the disposal of cryptoassets through gratuitous transfers (e.g., donations or inheritance) may be subject to stamp tax at a rate of 10 per cent, which is borne by the beneficiary of the transfer. However, the exemption currently applicable for gratuitous transfers of other assets in favour of certain beneficiaries (e.g., spouse, unmarried partner, descendants and ascendants) also applies to gratuitous transfers of cryptoassets.

For the assessment of the relevant value on which property transfer tax (PTT) should be levied whenever the purchase price of a given property is wholly or partially paid in cryptoassets, the value of the cryptoassets given in exchange, to be determined under the terms established in the Stamp Tax Code, should be taken into account.

Accordingly, the taxable value of cryptoassets is determined by taking into consideration the following rules, by the indicated order: (1) the specific rules provided for in the stamp tax code; (2) the value of the official quotation, when it exists; or (3) the value declared by the head of the estate (*cabeça-de-casal*) or by the beneficiary, and, as much as possible, should approximate the market value.

For the purposes of this last rule, if the Portuguese Tax Authority justifiably considers that there may be divergence between the value declared and the market value, it may determine the taxable value based on the market value.

iv Fourth block

The fourth block concerns the taxation of commissions and fees charged by cryptoasset service providers. Under the tax framework for cryptoassets, commissions and fees charged on transactions carried out by or with the intermediation of cryptoasset service providers domiciled in Portuguese territory or to customers domiciled^[15] in Portuguese territory are subject to a 4 per cent stamp tax rate, which is borne by the customers. In the event of non-payment, the customer will be jointly and severally liable with the service provider for the payment of the tax.

While the cryptoasset tax framework provides clarity on the taxation of cryptoasset transactions, it is silent on the value added tax (VAT) implications. Before this tax framework, the interpretation of the Court of Justice of the European Union (CJEU) and the binding rulings issued by the Portuguese Tax Authority (PTA)^[16] served as reference points to assess the VAT treatment of transactions with cryptoassets. In line with the CJEU interpretation of the VAT treatment of transactions with cryptocurrencies,^[17] the PTA ruled that transactions such as the exchange of cryptocurrency for fiat currency (and vice versa) should be exempt from VAT.^[18] While this guidance on the exemption for the exchange of cryptocurrencies for fiat currency, and vice versa, can still be relied on, the tax framework implies a different approach to the VAT treatment of transactions with cryptoassets. For now, it has become apparent that transactions with cryptoassets carried out in the course of a business or professional activity should be subject to VAT unless an exemption applies; for example, unless they qualify as transactions concerning currency, transactions in securities, transactions concerning negotiable instruments, among many other VAT exemptions provided for in the Portuguese VAT legislation transposing the VAT Directive.

Working Paper No. 1060, issued in February 2023 by the EU VAT Committee, on the VAT treatment of transactions involving NFTs, provides a good illustration of the complexity of determining whether a person or entity making transactions with cryptoassets is a taxable person or not, the nature and corresponding VAT treatment of transactions with cryptoassets, their place of supply and taxable amount, as well as on different criteria adopted by different EU Member States.

However, the full extent of the changes brought by the recent Portuguese tax framework for cryptoassets is yet to be determined. Thus, the practical application in the course of the next few years will be critical in gauging the impact of the new tax framework on the VAT treatment of transactions with cryptoassets.

Other new business models

The Portuguese fintech market has recently been experiencing great dynamism, with the entry of new players and stakeholders offering new types of services and products. We believe this dynamism will increase further when the new proposals for regulations under

the European Union's Digital Finance Package come to light, encouraging the continued growth of the market already fostered by the transposed PSD II and opening up new business opportunities for emerging companies in the areas of open banking services, neo-banks and all other innovation-driven solutions being developed in the banking and financial sector today.

However, in the meantime, new fintech companies offering innovative services may struggle with the burdensome procedures imposed by the applicable laws and regulations mentioned above (including the licence and registration procedures or AML-related issues), as well as the process of registering certain virtual assets activities with the BoP.

Despite the above, services resorting to smart contracts do seem to have some legal comfort. Since 2004, Portugal has had a specific provision dealing with contracts 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 the doctrine of mistake to programming errors, malfunctions and distorted messages. Although self-executing or smart contracts are a step further from contracts concluded without human intervention, it appears that they are permitted under Portuguese law; what is more, the above provision may be applicable to them. There is a general principle in Portuguese law that, unless otherwise provided, contracts are not subject to a specific form. However, no specific legal framework exists on smart contracts.

The past year has seen an increasing number of partnerships between banks and other non-regulated entities constituting consumer and merchant-friendly business models, working together on achieving the best consumer experience while at the same time working through the applicable legal and regulatory requirements on credit granting.

Artificial intelligence (AI) has also been widely adopted in fintech organisations in Portugal, particularly in the areas of customer service, fraud detection and risk management. One example is chatbots, which use natural language processing to provide customers with quick and efficient support. Another example is machine learning algorithms that can analyse vast amounts of data to detect fraudulent transactions and prevent financial crimes. Looking ahead, it is expected that AI will continue to play a significant role in the evolution of fintech in Portugal, particularly in areas such as credit scoring, investment management and personalised financial advice.

In this context, the proposed Artificial Intelligence Act (AI Act) which lays down harmonised rules on artificial intelligence, the final text of which has been recently endorsed by all EU member states, is expected to significantly impact the financial sector by introducing a risk-based approach to AI regulation, ensuring transparency, ethical use and accountability. Nonetheless, the AI Act allows for possible derogations by the Member States for reasons of national security, public security or for the protection of fundamental rights and freedoms, an implementing act will most likely be implemented by the Portuguese legislator.

Furthermore, the (proposed) AI liability directive which aims to establish clear rules for the responsible development and use of AI technologies could also have significant implications for the fintech industry. For example, fintech companies using AI for credit scoring or fraud detection will need to ensure that their algorithms are transparent, explainable and free from bias as well as to establish procedures for monitoring and auditing their AI systems to detect any errors or issues that could lead to harm.

In addition to the above, the European Supervisory Authorities have issued from 2015 onwards various reports on the use of AI in fintech and on automation in financial advice. In particular, (1) the EBA has issued guidelines on the use of AI and machine learning (ML) in the banking sector which provide recommendations for financial institutions on how to ensure responsible and ethical use of AI/ML in their business activities, including risk management, governance, and data management and (2) the ESMA's Final Report Guidelines on certain aspects of the MiFID II suitability requirements, published on 23 September 2022 following public consultation, includes specific recommendations to entities using AI to provide robo-advice, including obligations on the provision of minimum information to consumers and investors regarding the use of robo-advice, human intervention and the format that such information should be provided in.

The Cybersecurity Law (Law 46/2018) which transposed the NIS Directive (Directive (EU) 2016/1148) is the main legal instrument regulating cybersecurity in Portugal. However, the Cybersecurity Law in Portugal will be amended in the short to medium term to comply with the NIS 2 Directive (Directive (EU) 2022/2555). This will affect entities in the banking and financial market infrastructure sectors, which will need to comply with new obligations once the directive is transposed into national law.

The financial sector will further be impacted by the Digital Operational Resilience Act (DORA), which aims to ensure the operational resilience of digital services providers in the EU, including fintech companies and sets out requirements for IT systems, governance, and incident reporting to minimise the risk of disruption to services as well as CER, the Directive on the Resilience of Critical Entities, which focuses on resilience against physical risks. Overall, these regulations will increase the regulatory burden on the financial sector but also provide more clarity and stability for the fintech sector, which could help to increase investor confidence and encourage further innovation.

The Portuguese fintech market has recently been experiencing great dynamism, with the entry of new players and stakeholders offering new types of services and products. We believe this dynamism will increase further when the new proposals for regulations under the European Union's Digital Finance Package come to light, encouraging the continued growth of the market already fostered by the transposed PSD II and opening up new business opportunities for emerging companies in the areas of open banking services, neo-banks and all other innovation-driven solutions being developed in the banking and financial sector today.

However, in the meantime, new fintech companies offering innovative services may struggle with the burdensome procedures imposed by the applicable laws and regulations mentioned above (including the licence and registration procedures or AML-related issues), as well as the process of registering certain virtual assets activities with the BoP.

Despite the above, services resorting to smart contracts do seem to have some legal comfort. Since 2004, Portugal has had a specific provision dealing with contracts 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 the doctrine of mistake to programming errors, malfunctions and distorted messages. Although self-executing or smart contracts are a step further from contracts concluded without human intervention, it appears that they are permitted under Portuguese law; what is more, the above provision may be applicable to them. There is a general

principle in Portuguese law that, unless otherwise provided, contracts are not subject to a specific form. However, no specific legal framework exists on smart contracts.

The past year has seen an increasing number of partnerships between banks and other non-regulated entities constituting consumer and merchant-friendly business models, working together on achieving the best consumer experience while at the same time working through the applicable legal and regulatory requirements on credit granting.

Artificial intelligence (AI) has also been widely adopted in fintech organisations in Portugal, particularly in the areas of customer service, fraud detection and risk management. One example is chatbots, which use natural language processing to provide customers with quick and efficient support. Another example is machine learning algorithms that can analyse vast amounts of data to detect fraudulent transactions and prevent financial crimes. Looking ahead, it is expected that AI will continue to play a significant role in the evolution of fintech in Portugal, particularly in areas such as credit scoring, investment management and personalised financial advice.

In this context, the proposed Artificial Intelligence Act (AI Act) which lays down harmonised rules on artificial intelligence, the final text of which has been recently endorsed by all EU member states, is expected to significantly impact the financial sector by introducing a risk-based approach to AI regulation, ensuring transparency, ethical use and accountability. Nonetheless, the AI Act allows for possible derogations by the Member States for reasons of national security, public security or for the protection of fundamental rights and freedoms, an implementing act will most likely be implemented by the Portuguese legislator.

Furthermore, the (proposed) AI liability directive which aims to establish clear rules for the responsible development and use of AI technologies could also have significant implications for the fintech industry. For example, fintech companies using AI for credit scoring or fraud detection will need to ensure that their algorithms are transparent, explainable and free from bias as well as to establish procedures for monitoring and auditing their AI systems to detect any errors or issues that could lead to harm.

In addition to the above, the European Supervisory Authorities have issued from 2015 onwards various reports on the use of AI in fintech and on automation in financial advice. In particular, (1) the EBA has issued guidelines on the use of AI and machine learning (ML) in the banking sector which provide recommendations for financial institutions on how to ensure responsible and ethical use of AI/ML in their business activities, including risk management, governance, and data management and (2) the ESMA's Final Report Guidelines on certain aspects of the MiFID II suitability requirements, published on 23 September 2022 following public consultation, includes specific recommendations to entities using AI to provide robo-advice, including obligations on the provision of minimum information to consumers and investors regarding the use of robo-advice, human intervention and the format that such information should be provided in.

The Cybersecurity Law (Law 46/2018) which transposed the NIS Directive (Directive (EU) 2016/1148) is the main legal instrument regulating cybersecurity in Portugal. However, the Cybersecurity Law in Portugal will be amended in the short to medium term to comply with the NIS 2 Directive (Directive (EU) 2022/2555). This will affect entities in the banking and financial market infrastructure sectors, which will need to comply with new obligations once the directive is transposed into national law.

The financial sector will further be impacted by the Digital Operational Resilience Act (DORA), which aims to ensure the operational resilience of digital services providers in the EU, including fintech companies and sets out requirements for IT systems, governance, and incident reporting to minimise the risk of disruption to services as well as CER, the Directive on the Resilience of Critical Entities, which focuses on resilience against physical risks. Overall, these regulations will increase the regulatory burden on the financial sector but also provide more clarity and stability for the fintech sector, which could help to increase investor confidence and encourage further innovation.

Intellectual property and data protection

The protection of fintech can be carried out through several means. The protection of software seems to be the most relevant, as fintech technology usually translates into 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, which transposed Directive 91/250/CEE, later repealed by Directive 2009/24/CE, on computer programs, as amended). Copyright of a computer program belongs to the employer if the software is created by an employee in the execution of his or her duties or following instructions given by the employer. Copyright does not require a registry to exist, but this can be done in the General-Inspection for Cultural Activities. Software can also be protected by patent in cases where it meets the criteria to be considered a computer-implemented invention (i.e., an invention whose implementation involves the use of a computer, computer network or other programmable apparatus). In addition, computer-implemented business models can also be patented, to the extent that they are claimed as a technical solution for a technical problem (e.g., automating a response to the data collected) and involve technical considerations (e.g., the reading of a database). Otherwise, business models are not patentable. All in all, a case-by-case analysis is necessary to determine if protection by patent is feasible.

Technology developed in the context of a fintech business can also be protected as a trade secret. Trade secrecy protects against any act of a person who accesses, appropriates or copies (or any other conduct that, under the circumstances, is considered contrary to honest commercial practices), without consent, information that is secret, that has a commercial value because of that fact and that has been subject to reasonable steps, by the person lawfully in control of the information, to keep it secret (for instance, the execution of non-disclosure agreements). Current national legal provisions on trade secrecy are included in the Industrial Property Code, approved by Decree-Law No. 110/2018 of 10 December 2018, as reviewed following the transposition of Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

A computer platform usually comprises a set of data, as well as visual interfaces. This data may also be protected as a database if the requirements set forth by law (namely, Decree-Law No. 122/2000, which transposed Directive 96/9/CE, as amended, on the protection of databases) are met. Interfaces can be further protected by copyright under the Copyright Code (approved by Decree-Law No. 63/85, as amended) in what respects their look and feel, screen display and individual visual elements, if they all meet the criteria to be protected (mainly, are 'creative'). Copyright protection, in this case, belongs to the employer

or the person that ordered the creation, if so established or if the name of the creator is not referred to in the work. In this case, the creator may require special compensation if the creation exceeds the performance of the task set or when the creation is used in a way or brings benefits not included or foreseen in the creator's remuneration.

Fintech businesses collect, control and process vast amounts of personal data (including KYC data) and, as a result, they are subject to the data privacy rules provided in the General Data Protection Regulation (GDPR), which 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 and the processing of the customers' personal data is made in the context of the offering of services to those data subjects, irrespective of whether a payment is required from the data subject. The European Data Protection Board (EDPB) has clarified, in its Guidelines 3/2018 on the territorial scope of the GDPR, adopted on 16 November 2018, that the intention to target customers in the EU is key to assessing whether entities established outside the territory of the EU are subject to the GDPR.

In some instances, the processing of personal data may require the customer's consent. Pre-ticked opt-in or opt-out boxes will no longer be allowed, as consent must be expressed through a statement or clear affirmative action. The GDPR places onerous accountability obligations on data controllers to evidence compliance, which constitutes a major paradigm shift in the data protection regime. This includes the conduct of data protection impact assessments for more risky processing operations (such as those involving the processing of personal data that could be used to commit financial fraud) and the implementation of data protection by design and by default.

These general data protection rules are complemented by banking secrecy and AML rules, which fintech companies will have to observe when providing services to their clients.

Bank secrecy rules determine that the disclosure of clients' personal data protected by banking secrecy (including cross-border transfers) is permitted only with the client's prior authorisation or if the disclosure is necessary to achieve one of the following:

1. compliance with a legal obligation that expressly limits those secrecy duties;
2. compliance with judicial authorities' requests in the context of criminal proceedings;
or
3. compliance with a disclosure obligation towards the BoP, the CMVM or the tax authorities, when these entities are acting pursuant to their respective attributions.

In the past, the Portuguese Data Protection Authority (CNPD) had ruled in a specific case that all personal data processed by a bank is subject to banking secrecy.

As regards the processing of clients' data for the purposes of AML reporting, the disclosure of specific relevant personal data is based upon the fulfilment of a legal obligation, and there is thus no need to obtain the data subject's consent. As the concept of 'client authorisation' under the PSEMLF and the financial institutions' legal framework differs from the concept of 'consent' under the GDPR, many banks and other financial institutions opt to collect clients' authorisation to disclose information covered by banking secrecy in the context of their general client terms and conditions.

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 that produce effects concerning the data subject or that significantly affect them and are based solely on the automated processing of data intended to evaluate certain personal aspects relating to them are not permitted.

The GDPR has introduced new provisions to address the risks arising from profiling and automated decision-making. Mainly, under the GDPR, one may only carry out this type of decision-making where the decision is either necessary for the entry into or performance of a contract or authorised by the EU or Member State law applicable to the controller, or, finally, based on the individual's explicit consent. Where one of these grounds applies, additional safeguards must be introduced, as well as disclosure of specific information about automated individual decision-making to affected data subjects, concerning the logic, significance and envisaged consequences. In a January 2020 response to the Member of the European Parliament Sophie in 't Veld's letter on unfair algorithms, addressing whether the GDPR was sufficient to protect data subjects from unfair automated decision-making, the EDPB stressed that 'controllers are obliged to consider all the potential risks that the use or creation of the specific algorithm can potentially pose to the rights and freedoms of natural persons and, if necessary, take measures to address these risks'.

There are also 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 PSD II Regulatory Technical Standards, as the Regulatory Technical Standards suggest the use of the payment service users' biometric data in that context. The CNPD has consistently ruled that financial data are sensitive data, in the sense that they reveal aspects of an individual's private life and, therefore, should be protected under the Portuguese Constitution. As financial data is also considered by the EDPB as data of a highly personal nature, this may ultimately influence the stringency of technical and organisational measures that data controllers and processors choose to implement to protect the data, as well as the need to undergo a data protection impact assessment (DPIA) before commencing processing activities on the data. The processing of financial data may, then, entail the need for a DPIA under the CNPD's Regulation 1/2018, which lists the processing activities that are subject to a mandatory DPIA, as the Regulation refers to the processing of data of a highly personal nature in four of its nine cases.

Without prejudice to the above, Portuguese legislation implementing the GDPR entered into force on 8 August 2019. Law No. 58/2019 brings some additional adjustments and restrictions to the rules set out in the GDPR, notably regarding the processing of deceased persons' personal data, the applicable data storage periods and minors' consent for data processing. Most notably, and without prejudice to the GDPR's purpose limitation principle, Law No. 58/2019 allows controllers or processors to keep personal data until the expiry of any statutory limitation periods during which they may need to use the data to demonstrate compliance with legal or contractual obligations.

The EDPB, in particular Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions and Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the

GDPR, specifically referring to finance data and payment service providers in particular, should also be taken into consideration in this context.

The protection of fintech can be carried out through several means. The protection of software seems to be the most relevant, as fintech technology usually translates into 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, which transposed Directive 91/250/CEE, later repealed by Directive 2009/24/CE, on computer programs, as amended). Copyright of a computer program belongs to the employer if the software is created by an employee in the execution of his or her duties or following instructions given by the employer. Copyright does not require a registry to exist, but this can be done in the General-Inspection for Cultural Activities. Software can also be protected by patent in cases where it meets the criteria to be considered a computer-implemented invention (i.e., an invention whose implementation involves the use of a computer, computer network or other programmable apparatus). In addition, computer-implemented business models can also be patented, to the extent that they are claimed as a technical solution for a technical problem (e.g., automating a response to the data collected) and involve technical considerations (e.g., the reading of a database). Otherwise, business models are not patentable. All in all, a case-by-case analysis is necessary to determine if protection by patent is feasible.

Technology developed in the context of a fintech business can also be protected as a trade secret. Trade secrecy protects against any act of a person who accesses, appropriates or copies (or any other conduct that, under the circumstances, is considered contrary to honest commercial practices), without consent, information that is secret, that has a commercial value because of that fact and that has been subject to reasonable steps, by the person lawfully in control of the information, to keep it secret (for instance, the execution of non-disclosure agreements). Current national legal provisions on trade secrecy are included in the Industrial Property Code, approved by Decree-Law No. 110/2018 of 10 December 2018, as reviewed following the transposition of Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

A computer platform usually comprises a set of data, as well as visual interfaces. This data may also be protected as a database if the requirements set forth by law (namely, Decree-Law No. 122/2000, which transposed Directive 96/9/CE, as amended, on the protection of databases) are met. Interfaces can be further protected by copyright under the Copyright Code (approved by Decree-Law No. 63/85, as amended) in what respects their look and feel, screen display and individual visual elements, if they all meet the criteria to be protected (mainly, are 'creative'). Copyright protection, in this case, belongs to the employer or the person that ordered the creation, if so established or if the name of the creator is not referred to in the work. In this case, the creator may require special compensation if the creation exceeds the performance of the task set or when the creation is used in a way or brings benefits not included or foreseen in the creator's remuneration.

Fintech businesses collect, control and process vast amounts of personal data (including KYC data) and, as a result, they are subject to the data privacy rules provided in the General Data Protection Regulation (GDPR), which 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 and the processing of the customers' personal data is made in

the context of the offering of services to those data subjects, irrespective of whether a payment is required from the data subject. The European Data Protection Board (EDPB) has clarified, in its Guidelines 3/2018 on the territorial scope of the GDPR, adopted on 16 November 2018, that the intention to target customers in the EU is key to assessing whether entities established outside the territory of the EU are subject to the GDPR.

In some instances, the processing of personal data may require the customer's consent. Pre-ticked opt-in or opt-out boxes will no longer be allowed, as consent must be expressed through a statement or clear affirmative action. The GDPR places onerous accountability obligations on data controllers to evidence compliance, which constitutes a major paradigm shift in the data protection regime. This includes the conduct of data protection impact assessments for more risky processing operations (such as those involving the processing of personal data that could be used to commit financial fraud) and the implementation of data protection by design and by default.

These general data protection rules are complemented by banking secrecy and AML rules, which fintech companies will have to observe when providing services to their clients.

Bank secrecy rules determine that the disclosure of clients' personal data protected by banking secrecy (including cross-border transfers) is permitted only with the client's prior authorisation or if the disclosure is necessary to achieve one of the following:

1. compliance with a legal obligation that expressly limits those secrecy duties;
 2. compliance with judicial authorities' requests in the context of criminal proceedings;
- or
3. compliance with a disclosure obligation towards the BoP, the CMVM or the tax authorities, when these entities are acting pursuant to their respective attributions.

In the past, the Portuguese Data Protection Authority (CNPD) had ruled in a specific case that all personal data processed by a bank is subject to banking secrecy.

As regards the processing of clients' data for the purposes of AML reporting, the disclosure of specific relevant personal data is based upon the fulfilment of a legal obligation, and there is thus no need to obtain the data subject's consent. As the concept of 'client authorisation' under the PSEMLF and the financial institutions' legal framework differs from the concept of 'consent' under the GDPR, many banks and other financial institutions opt to collect clients' authorisation to disclose information covered by banking secrecy in the context of their general client terms and conditions.

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 that produce effects concerning the data subject or that significantly affect them and are based solely on the automated processing of data intended to evaluate certain personal aspects relating to them are not permitted.

The GDPR has introduced new provisions to address the risks arising from profiling and automated decision-making. Mainly, under the GDPR, one may only carry out this type of decision-making where the decision is either necessary for the entry into or performance of a contract or authorised by the EU or Member State law applicable to

the controller, or, finally, based on the individual's explicit consent. Where one of these grounds applies, additional safeguards must be introduced, as well as disclosure of specific information about automated individual decision-making to affected data subjects, concerning the logic, significance and envisaged consequences. In a January 2020 response to the Member of the European Parliament Sophie in 't Veld's letter on unfair algorithms, addressing whether the GDPR was sufficient to protect data subjects from unfair automated decision-making, the EDPB stressed that 'controllers are obliged to consider all the potential risks that the use or creation of the specific algorithm can potentially pose to the rights and freedoms of natural persons and, if necessary, take measures to address these risks'.

There are also 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 PSD II Regulatory Technical Standards, as the Regulatory Technical Standards suggest the use of the payment service users' biometric data in that context. The CNPD has consistently ruled that financial data are sensitive data, in the sense that they reveal aspects of an individual's private life and, therefore, should be protected under the Portuguese Constitution. As financial data is also considered by the EDPB as data of a highly personal nature, this may ultimately influence the stringency of technical and organisational measures that data controllers and processors choose to implement to protect the data, as well as the need to undergo a data protection impact assessment (DPIA) before commencing processing activities on the data. The processing of financial data may, then, entail the need for a DPIA under the CNPD's Regulation 1/2018, which lists the processing activities that are subject to a mandatory DPIA, as the Regulation refers to the processing of data of a highly personal nature in four of its nine cases.

Without prejudice to the above, Portuguese legislation implementing the GDPR entered into force on 8 August 2019. Law No. 58/2019 brings some additional adjustments and restrictions to the rules set out in the GDPR, notably regarding the processing of deceased persons' personal data, the applicable data storage periods and minors' consent for data processing. Most notably, and without prejudice to the GDPR's purpose limitation principle, Law No. 58/2019 allows controllers or processors to keep personal data until the expiry of any statutory limitation periods during which they may need to use the data to demonstrate compliance with legal or contractual obligations.

The EDPB, in particular Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions and Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, specifically referring to finance data and payment service providers in particular, should also be taken into consideration in this context.

Outlook and conclusions

It was expected that crowdfunding investment schemes would have increased in terms of both the number of entities operating in the market and the transaction volume associated with these types of investments, but that does not seem to be the case just yet.

The envisaged new regulation on the cryptocurrencies market (MiCA) is also promising, but its biggest challenge may be the jurisdiction cherry-picking process pursuant to which market entrants will make their decisions based on which regulator they expect to be the speedier and friendlier one.

It is difficult to provide an exact number of token and security-related businesses opening in Portugal, as data on this topic is limited. However, it is clear that the country has been attracting a growing number of blockchain and cryptoasset-related businesses in recent years and is expected to continue taking into consideration Portugal's relatively friendly regulatory environment.

Finally, the Portuguese government continues to expect ZLTs to boost international projects, attract foreign investment and position the country as an international research, development and innovation leader, which will surely benefit and contribute to the stimulation of the fintech ecosystem.

It was expected that crowdfunding investment schemes would have increased in terms of both the number of entities operating in the market and the transaction volume associated with these types of investments, but that does not seem to be the case just yet.

The envisaged new regulation on the cryptocurrencies market (MiCA) is also promising, but its biggest challenge may be the jurisdiction cherry-picking process pursuant to which market entrants will make their decisions based on which regulator they expect to be the speedier and friendlier one.

It is difficult to provide an exact number of token and security-related businesses opening in Portugal, as data on this topic is limited. However, it is clear that the country has been attracting a growing number of blockchain and cryptoasset-related businesses in recent years and is expected to continue taking into consideration Portugal's relatively friendly regulatory environment.

Finally, the Portuguese government continues to expect ZLTs to boost international projects, attract foreign investment and position the country as an international research, development and innovation leader, which will surely benefit and contribute to the stimulation of the fintech ecosystem.

Endnotes

- 1 Tiago Correia Moreira is a partner, Conceição Gamito is a senior counsel, Helena Correia Mendonça is a principal consultant and David Paula is a senior associate at Vieira de Almeida. The authors would like to thank Ana Falcão Afonso, a principal consultant in the IP department, for her assistance with the chapter. [^ Back to section](#)

- 2 In this respect, it is noteworthy that Directive (EU) 2015/1535 of the European Parliament and of the Council, which defines and sets out rules for information society services, states that this Directive shall not apply to rules relating to matters covered by EU legislation in the field of financial services, as non-exhaustively listed in Annex II to this Directive. This may ultimately raise some doubts about the applicability of Regulation (EU) 2019/1150 to the provision of online intermediation services relating to financial services. The Regulation also states that it 'shall not apply to online payment services . . . which are not provided with the aim of facilitating the initiation of direct transactions and which do not involve a contractual relationship with consumers', without prejudice to EU law applicable in the areas of judicial cooperation in civil matters, competition, data protection, trade secrets protection, consumer protection, electronic commerce and financial services. [^ Back to section](#)
- 3 Following a study carried out by the European Central Bank on 'Virtual Currency Schemes', from October 2012. In 2014, the Bank of Portugal also reiterated that the use of virtual currency brings risks to consumers and, in 2015, it advised banks to abstain from buying, detaining or selling virtual currencies (Circular Letter 011/2015/DPG of 10 March 2015). [^ Back to section](#)
- 4 See ESMA, 'Advice: Initial Coin Offerings and Crypto-Assets', published on 9 January 2019 (ESMA50-157-1391). [^ Back to section](#)
- 5 The MiCA Regulation, which will establish harmonised rules for cryptoassets at EU level, aims at providing legal certainty for cryptoassets not covered by existing EU legislation and will shortly be voted by the European Parliament. See Markets in Cryptoassets (MiCA) (europa.eu). [^ Back to section](#)
- 6 Directive Council Directive (EU) 2023/2226 of 17 October 2023 (DAC 8) amending Directive 2011/16/EU on administrative cooperation in the field of taxation, entered into force on 13 November 2023. EU Member States must transpose the DAC 8 by 31 December 2025, which will be applicable from 1 January 2026 with certain exceptions. These amendments are aimed at improving Member States' ability to detect and counter tax fraud, tax evasion and tax avoidance, by requiring all cryptoasset service providers to report transactions of clients residing in the European Union. [^ Back to section](#)
- 7 Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax. [^ Back to section](#)
- 8 Council Implementing Regulation (EU) No. 282/2011 of 15 March 2011 laying down implementing measures for the VAT Directive. [^ Back to section](#)
- 9 Regime generally applicable to PIT taxpayers who, in the course of their business, have not exceeded a gross annual amount of Category B income of €200,000 in the previous tax period. [^ Back to section](#)

- 10** Regime applicable to PIT taxpayers who, in the course of their business, have exceeded a gross annual amount of Category B income of €200,000 in the previous tax period. [^ Back to section](#)
- 11** A solidarity surcharge of (1) 2.5 per cent applies to taxable income exceeding €80,000, up to €250,000 and (2) 5 per cent to taxable income exceeding €250,000. [^ Back to section](#)
- 12** Cryptoassets that qualify as securities should be taxable as securities. [^ Back to section](#)
- 13** €81,199.00. [^ Back to section](#)
- 14** Optional regime for the determination of the taxable base applicable to entities that, in the previous tax period, have obtained an annual gross income not exceeding €200,000, whose balance sheet for the immediately preceding tax period does not exceed €500,000 and are not legally required to have statutory audits. [^ Back to section](#)
- 15** Namely with residence, head office, effective management, subsidiary, branch or permanent establishment in Portuguese territory. [^ Back to section](#)
- 16** Binding Rulings 12904 of 15 February 2018 and 14763 of 28 January 2019. [^ Back to section](#)
- 17** Court of Justice of the European Union (CJEU) Case C-264/14, 22 October 2015 (*Skatteverket v. David Hedqvist*). In this case, the CJEU decided that the exchange of Bitcoin for traditional currency qualifies as a supply of services for VAT purposes. As to the question of whether these transactions should be regarded as exempt supplies, the CJEU pointed out that Bitcoin, being a contractual means of payment, cannot be regarded as a current account or a deposit account, a payment or transfer. Moreover, unlike a debt, cheques and other negotiable instruments referred to in Article 135(1)(d) of the VAT Directive, Bitcoin is a direct means of payment between the operators that accept it. Therefore, the CJEU ruled that transactions such as the exchange of cryptocurrency for traditional currency, and vice versa, should be exempt from VAT under the provision of Article 135(1)(e) of the VAT Directive. The CJEU did not expressly address the subject of whether the exchange of, for example, Bitcoin for a different cryptocurrency should also be regarded, for VAT purposes, as an exempt supply of services under Article 135(1)(e) of the VAT Directive. However, in our view, the same reasoning applies and the answer should therefore be the same. [^ Back to section](#)
- 18** Under Article 9(27)(d) of the Portuguese VAT Code (which corresponds to the transposition of Article 135(1)(e) of the European VAT Directive). [^ Back to section](#)



Tiago Correia Moreira
Conceição Gamito
Helena Correia Mendonça
David Paula

tcm@vda.pt
crg@vda.pt
hcm@vda.pt
dcp@vda.pt

Vieira de Almeida & Associados

[Read more from this firm on Lexology](#)