

Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering
comparative analysis from top ranked lawyers

FinTech

Spain
finReg360

chambers.com

2019

Law and Practice

Contributed by finReg360

Contents

1. FinTech Market	p.5	7. Exchanges and Trading Platforms	p.11
1.1 Evolution of the FinTech Market	p.5	7.1 Permissible Trading Platforms	p.11
2. FinTech Verticals	p.5	7.2 Regulation of Different Asset Classes	p.11
2.1 Predominant Business Models	p.5	7.3 Impact of the Emergence of Cryptocurrency Exchanges	p.12
2.2 Regulatory Regime	p.5	7.4 Listing Standards	p.12
2.3 Variations Between the Regulation of FinTech and Legacy Players	p.6	7.5 Order-handling Rules	p.12
2.4 Regulatory Sandbox	p.6	7.6 Rise of Peer-to-Peer Trading Platforms	p.13
2.5 Jurisdiction of Regulators	p.7	7.7 Issues Relating to Best Execution of Customer Trades	p.13
2.6 Outsourcing of Regulated Functions	p.7	7.8 Rules of Payment for Order Flow	p.13
2.7 Significant Enforcement Actions	p.7	8. High-frequency and Algorithmic Trading	p.13
2.8 Implications of Additional Regulation	p.7	8.1 Creation and Usage Regulations	p.13
2.9 Regulation of Social Media and Similar Tools	p.8	8.2 Exchange-like Platform Participants	p.13
2.10 Review of Industry Participants by Parties Other Than Regulators	p.9	8.3 Requirement to Register as Market Makers When Functioning in a Principal Capacity	p.13
2.11 Conjunction of Unregulated and Regulated Products and Services	p.9	8.4 Issues Relating to the Best Execution of Trades	p.13
3. Robo-advisers	p.9	8.5 Regulatory Distinction Between Funds and Dealers	p.14
3.1 Requirement for Different Business Models	p.9	8.6 Rules of Payment for Order Flow	p.14
3.2 Legacy Players' Implementation of Solutions Introduced by Robo-advisers	p.9	9. Financial Research Platforms	p.14
3.3 Issues Relating to Best Execution of Customer Trades	p.9	9.1 Registration	p.14
4. Online Lenders	p.9	9.2 Regulation of Unverified Information	p.14
4.1 Differences in the Business or Regulation of Loans Provided to Different Entities	p.9	9.3 Conversation Curation	p.14
4.2 Underwriting Processes	p.10	9.4 Platform Providers as 'Gatekeepers'	p.14
4.3 Sources of Funds for Loans	p.10	10. InsurTech	p.14
4.4 Syndication of Loans	p.11	10.1 Underwriting Processes	p.14
5. Payment Processors	p.11	10.2 Treatment of Different Types of Insurance	p.14
5.1 Payment Processors' Use of Payment Rails	p.11	11. RegTech	p.15
6. Fund Administrators	p.11	11.1 Regulation of RegTech Providers	p.15
6.1 Regulation of Fund Administrators	p.11	11.2 Contractual Terms to Assure Performance and Accuracy	p.15
6.2 Contractual Terms	p.11	11.3 RegTech Providers as 'Gatekeepers'	p.15
6.3 Fund Administrators as 'Gatekeepers'	p.11		

12. Blockchain	p.15
12.1 Use of Blockchain in the Financial Services Industry	p.15
12.2 Local Regulators' Approach to Blockchain	p.15
12.3 Classification of Blockchain Assets	p.15
12.4 Regulation of 'Issuers' of Blockchain Assets	p.16
12.5 Regulation of Blockchain Asset-trading Platforms	p.16
12.6 Regulation of Invested Funds	p.16
12.7 Virtual Currencies	p.17
12.8 Impact of Privacy Regulation on Blockchain	p.17
13. Open Banking	p.18
13.1 Regulation of Open Banking	p.18
13.2 Concerns Raised by Open Banking	p.18

finReg360 has become a reference consultancy firm in the financial sector, providing advice to Spanish and European financial and non-financial institutions, including market infrastructures, credit institutions, banks, insurance companies, market distributors, payment and e-money institutions and asset managers. Additionally, finReg has accompanied newly created FinTech firms (especially, open banking entities, payment institutions, securities brokers and robo-advisers) through their authorisation process to ensure that their business model is compliant with the regulation. The firm provides regulatory advice to all exist-

ing FinTech verticals due to the scope and nature of their services and is the trusted adviser of several of the most representative FinTech companies in Spain. Key practice areas include banking (including lending), payment services, investment funds, securities, insurance, anti-money laundering and counter-terrorism financing, information technology and data protection, and intellectual property. Furthermore, finReg is one of the promoters of Alastria, the first consortium for the establishment of a semi-public blockchain structure in Spain.

Authors



Sara Gutiérrez Campiña is a partner at the firm. She is an expert in the implementation of financial regulation with more than 15 years of experience in providing advice to financial entities. She has wide experience in implementing

projects of MiFID, PSD2, AIFMD, UCITS, IDD and MAR as well as supporting FinTech entities in defining their business models according to those regulations.

Additionally, Sara has been engaged in the creation of financial entities and FinTechs, restructuring of financial groups, drafting of contracts and she has advised financial entities in CNMV inspections. A speaker at many conferences on financial regulation and FinTech issues, Sara also collaborates with specialised journals relating to financial regulation. She is a member of the Madrid Bar Association, Fundación de Estudios Financieros and the Spanish Association of Compliance (ASCOM).



Jorge Ferrer Barreiro is a partner at the firm. He is an expert in private banking, UCITS, AIFMD, MiFID, PSD 2, AML/CTF and FinTech with more than 15 years' experience in financial regulation, advising financial institutions in the field

of investment services, asset management, venture capital and private banking. He also has wide experience in business strategic consultancy to adapt new business models to financial regulation (payment entities, robo-advisers, crowd-funding platforms, exchanges). Jorge also advises SMEs in capital raising processes. He is a member of the Madrid Bar Association and vice-president of the Spanish Association of Tokens and ICOs (AETOK); he is also a regular speaker at legal conferences on financial services regulation.



José María Olivares is a partner at finReg. His main areas of expertise are AML/CTF, banking and payment services (including PSD2 and the EMDs). He has more than 17 years' experience advising financial and non-financial institutions as well as

leading cross-border projects. As part of his experience, José regularly advises financial institutions in matters related to FinTech. He is a lecturer at ESADE Business & Law School (banking and financial institutions) as well as being a speaker at the legal module of the MiB2019 (Master on Internet Business) run by ISDI, the Instituto Superior para el Desarrollo de Internet. A member of the Madrid Bar Association, José regularly participates in seminars and conferences, most recently as a speaker in the seminars arranged by FIDE, a Spanish legal and economic think-tank of which finReg is a member, on matters such as the reality of cryptocurrencies and their regulation.



María Vidal is currently of counsel at finReg, and co-leads the TMT Group. María has 16 years of experience in information technology law and data protection. She has spent most of her career at Deloitte Legal, leading

international technology projects. Her key practice areas are data protection, IT agreements/web pages/e-marketing, advice on intellectual property rights, defence before the courts (appealing the decisions of the Spanish Data Protection Authority), training services – regulatory training of staff and senior management on GDPR, e-privacy, business strategic consultancy on data protection regulation in the development of new activities, especially for financial institutions. She is a member of the Madrid Bar Association and of ASCOM (the Spanish Association of Regulatory Compliance), and an accredited CIPP/E (Certified Information Privacy Professional/Europe) by the IAPP (International Association of Privacy Professionals). María is a speaker at many conferences on data protection, and has a wide range of lecturing and publishing credits to her name.

1. FinTech Market

1.1 Evolution of the FinTech Market

During the last 12 months we have seen a significant evolution in the verticals for payments, robo-advisers, InsurTech and RegTech, with RegTech being commonly used to cover obligations derived from the regulations on anti-money laundering and counter-terrorism financing (AML & CTF). The use of big data has also been affected by the entry into force of the new data protection legislation, which has changed the existing obligations in relation to obtaining consent. During that same period the rise of blockchain technology has brought with it new business models as well as a challenge for regulators, in terms of how blockchain-based products and services must or can be adapted to the existing legislation.

In Spain, the arrival of the regulatory sandbox is expected during the next few months. This will allow innovative companies to make use of a controlled testing environment, and will surely contribute to increased innovation and competitiveness for the financial industry in Spain.

2. FinTech Verticals

2.1 Predominant Business Models

FinReg provides specialised advice on financial regulation, including the following areas of the financial sector:

- the banking area and all legislation that affects credit institutions, banks, payment institutions, electronic money institutions, financing credit establishments, etc;
- legislation applicable to securities markets and their infrastructure, and the provision of investment services by regulated entities (for example, companies that provide investment services or manage collective investment schemes, crowdfunding entities, etc); and
- the insurance area, applicable to insurance companies as well as to distributors, intermediaries, websites that compare insurance products, etc.

In addition, FinReg provides specialised services on anti-money laundering and counter-terrorism financing obligations as well as on data protection requirements since these regulations are applicable to the provision of any financial services with major impact in terms of onboarding processes.

This specialisation allows us to provide guidance to entities that are taking advantage of technological advances and the changes being seen in consumer demands. They are offering digital solutions and reinventing the financial services being offered, by making them more efficient or by creating new models, while still being subject to supervision based on the applicable legislation.

Legal advice on FinTech (banking and investment areas) and InsurTech (insurance area) consists of providing guidance to these companies, for their understanding and compliance with the regulation.

Also noteworthy is the growing presence of robo-advisers, probably due to the increasing use of algorithms and the need to reduce the costs associated with investment advice processes (see also below, section 3. **Robo-advisers**). We are also seeing the arrival of websites that compare insurance products that provide added value for consumers. In the investment services area and with the entry into force of Directive (EU) 2014/65 on markets in financial instruments (MiFID II), one of the aspects that has most heavily affected traditional banks and that has forced them to revise their business models in relation to providing investment advice and discretionary portfolio management services, has been the incentives inducements system. In many cases these changes have required firms to invest in technology to ensure compliance with requirements on inducements and to reduce operating costs to balance the reduction of margins caused by the regulation.

There is also a discernible change in models where a substantial portion of the financial services provided are being integrated into a single channel. This includes everything from account aggregation services for both payments and securities to the possibility of recommending multiple products (loans, savings or investment products, insurance, etc) based upon a customer's profile. This has led to a shift in models at some entities, while also influencing the rise of the so-called 'neo-banks'. All of them, given their reliance on data management for support – which has also led to an increase in the use of big data – have been enormously affected by the new data protection legislation. In relation to this we would also like to emphasise the growth of solutions involving artificial intelligence, analysis of big data, outsourcing, and use of cloud computing. These are all solutions that, among others, are being impacted by financial regulation in terms of the activities being presented in these ways.

Finally, the veritable avalanche of legislation that the financial sector has been subject to in recent years, which has significantly expanded the regulatory obligations imposed upon these entities, when combined with technological advances, has given rise to RegTech, which is spurring the development of tools designed to make regulatory compliance more agile and flexible while also reducing costs, among other advantages.

2.2 Regulatory Regime

In general, the applicable legislation in Spain is defined at European level based upon the services or products being provided, and regardless of whether or not they are being offered by means of FinTech or InsurTech. This trend can be seen in almost all the verticals, with variation in the appli-

cable legislation depending upon the service provided. This means that, in general: investment services are regulated by MiFID II; insurance distribution services are regulated by Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (IDD); and payment services are regulated by Directive (EU) 2015/2366 on payment services in the internal market (PSD2). Nevertheless, and as mentioned above, entities that carry out these activities are subject to the same legislation regardless of whether or not they are based on FinTech or InsurTech technologies, and therefore by application of the principle of proportionality, the legislation may have a lesser impact on their business simply based upon the size of the entities themselves. It is also important to point out that although almost the entire regulatory system applicable to financial institutions is derived from European legislation, there are still some specificities.

In addition, given the absence of EU legislation on the subject, loans and platforms based on bringing together investors and companies seeking financing (crowdfunding in its equity and lending modalities) is regulated in Spain by local legislation.

There is also a lack of specific regulation for services provided via blockchain technology and services involving cryptoassets, so for the time being the general securities market legislation is being applied to them.

Finally, and as will be further detailed throughout this guide, the cross-cutting European legislation on AML & CTF and on data protection applies to all the verticals.

2.3 Variations Between the Regulation of FinTech and Legacy Players

The applicable legislation is the same for traditional participants and for those making use of FinTech or InsurTech. The European Commission's position is based upon three principles: (i) technological neutrality, to guarantee that the same activity will be subject to the same regulation regardless of the manner in which a service is provided; (ii) proportionality; and (iii) integrity, since application of technologies to financial services should promote greater transparency in the market, to the benefit of consumers and without creating unjustified risks.

Meanwhile, in its preliminary observations the European Banking Authority (EBA) is stating that FinTech and InsurTech are regulated in conformity with the EU legislation. However, some models may remain outside of the current regimes, with authorisation or registration being governed by the contents of national legislation. This point will be addressed in further detail later, especially in sections **7. Exchanges and Trading Platforms** and **12 Blockchain**.

2.4 Regulatory Sandbox

In Spain the government has published draft legislation on measures related to the digital transformation. Its objective is to encourage innovation while also ensuring that the digital transformation does not reduce the levels of protection offered to consumers of financial services or affect financial stability or the integrity of the markets. Any measures that could facilitate use of the financial system for money laundering or financing of terrorism must also be avoided. This demonstrates Spain's willingness to respond to these needs, which represent a structural change, by facilitating technology-based financial innovation while also strengthening legal security, ensuring protection for those investing in financial services, and expanding the tools that regulators have available when carrying out their duties.

The principal features of the regulatory sandbox addressed in that draft legislation are the following:

- it is a controlled space (ie, a space that is safe for participants and without risk for the financial system as a whole) – entry into the sandbox will in no case involve obtaining authorisation to exercise the activity or to provide services that are typically considered as professional in nature;
- it is a supervisory tool; and
- it is governed by a law-protocol scheme.

As far as the regime for entering the sandbox, a financial one-stop system is being established for submission of projects. A technology firm, financial institution, research centre or any other interested sponsor can present a sufficiently well-advanced project, and it will be accepted as long as it has first received a favourable evaluation from the relevant authorities, based on their belief that it can provide added value. This means that it must comply with certain aspects, which may include improving regulatory compliance, the tools available for customer protection or increasing efficiency or otherwise enhancing the provision of financial services.

Following that evaluation, a protocol for performance of the testing must be developed by collaboration between the regulatory authorities and the sponsor, and it must include details on the tests to be performed, such as their duration and scope. Once the protocol has been established the testing can begin, as long as the requested guarantees are in place. These are especially strict in cases where customers will be participating: informed consent and data protection; the right of withdrawal at any time; liability of the sponsor if any monetary losses directly result from performance of the tests; a guarantee to cover compensation for such losses; confidentiality; monitoring by the regulatory authority during execution of all tests; and finally, the possibility of suspending the testing under circumstances that include,

among others, abusive or negligent practices or violations of the applicable legislation or protocol.

In terms of the exit regime, there are three elements included:

- examination of the results, which must be performed by the sponsor of the testing and then included in a report submitted to the regulatory authorities that have been monitoring the tests;
- the pathway for obtaining the licence, which presents a substantial reduction of the procedures required in cases where licensing for the activity has not existed up until that time;
- application of proportionality.

Although no exact date has been confirmed, it is expected that Spain's sandbox will go into operation in 2019.

In this context, it is worth emphasising that the EBA has already shown concern regarding the different approaches being used by national authorities in the European Union with regard to their sandboxes, and it is likely that this will give rise to regulatory arbitration and other problems, thereby presenting risks for consumers.

2.5 Jurisdiction of Regulators

In Spain there are three regulators that cover the following areas:

- for aspects related to investment markets and services, the competent regulatory authority is the National Securities Market Commission (*Comisión Nacional del Mercado de Valores*, CNMV);
- for matters related to banking and credit institutions, the Bank of Spain (BdE) is responsible for supervision; and
- insurance companies and pension funds and operations in these industries are supervised by the General Department of Insurance and Pension Funds (*Dirección General de Seguros y Fondos de Pensiones*, DGSFP).

In parallel, there is also legislation that applies to all these areas of activity, regardless of the nature of the activities involved:

- AML & CTF, with the relevant authority being the Executive Service for Prevention of Money Laundering (*Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias*, SEPBLAC);
- data protection, with the authority being the Spanish Data Protection Agency (*Agencia Española de Protección de Datos*, AEPD).

2.6 Outsourcing of Regulated Functions

Regulated entities that are outsourcing operational functions critical for a service must ensure that they are still able to provide the service in a continuous and satisfactory manner.

The company outsourcing these services must also perform any actions that may be required to prevent any additional operational risk.

Furthermore, the legislation prohibits any outsourcing that prevents the company's ability to monitor the service being outsourced, or that could affect the regulator's ability to ensure or verify that company's compliance with the legislation.

This brings up the need to include contractual clauses that give the company providing the service access to the information and data it needs in order to ensure compliance with its obligations in the event of an audit by the regulatory authority.

In the same way, and even though the regulated entity is still responsible for compliance, the provider of the outsourced service must comply with the obligations from the legislation, and no-recourse clauses can be established to cover cases where sanctions are applied in relation to any breaches attributable to that provider.

There are no regulatory restrictions that produce any requirement to outsource to a supervised entity, so in general that decision will depend upon the business model and the service being outsourced.

Finally, when outsourcing is taking place it must be ensured that provision of the service itself is not transferred to the technology supplier, although this has already occurred in some cases in the FinTech area such as with certain payment processors.

2.7 Significant Enforcement Actions

No significant sanctions have yet been imposed in Spain, but as the industry grows it is likely that sanctions will increase.

2.8 Implications of Additional Regulation

In Spain, both new entrants into the financial markets (FinTech and InsurTech) and traditional players are affected mainly by the following legislation:

- Spanish Organic Law 3/2018 of 5 December on Personal Data Protection and guarantees for digital rights (Spanish Personal Data Protection and Guarantees for Digital Rights Act);
- Royal Decree Law 12/2018 of 7 September on security for networks and information systems;
- Spanish Law 10/2010 of 28 April on prevention of money laundering and financing of terrorism;
- Royal Decree Law 19/2018 on payment services and other urgent measures on finance.

To avoid any actions likely to infringe these regulations, FinTech and InsurTech entrants, as well as the traditional play-

ers, must invest in regulatory compliance. However, it is easier for traditional financial entities already established in the market to assume the compliance-related costs, compared to the emerging FinTech and InsurTech entities. On the other hand, new regulations can also represent an opportunity for FinTech and InsurTech participants, since they are able to adapt more quickly to these new regulatory requirements. In fact, FinTech and InsurTech entities are more agile and flexible, mainly because of their size and because they do not have to transform and adjust an already established entire model. This means that FinTech and InsurTech entities can take these new legal requirements into account and apply them from the very beginning, which represents a competitive advantage compared to traditional entities. Indeed, traditional players are aware of this, and do not hesitate to offer, in a complementary manner, the FinTech and InsurTech products, which always tend to be more cutting-edge and more personalised for consumers.

In any event, Spain's regulatory framework will keep evolving in view of the public consultation launched by the Government in relation to the draft of a regulation promoting the start-up ecosystem, which aims to create a competitive and dynamic legal framework more favourable for start-up development.

2.9 Regulation of Social Media and Similar Tools

There is heavy regulation of social media in Spain, which is primarily derived from European directives and regulations. As in the rest of the EU Member States, that regulation is establishing the foundations for the single digital market, which the EU began to develop in 2015 as part of the Digital Agenda from the Europe 2020 Strategy.

The legislation developed in recent years that has affected social media sites has been focused on:

- guaranteeing free access to online products and services;
- establishing conditions for development of digital networks and services; and
- advancing Europe's digital economy.

As far as the strictly regulatory aspects, in the EU countries barriers such as geoblocking in relation to consumption of audiovisual products and e-commerce have been eliminated.

When focusing on social media it is essential to point out the repercussions of the application of the General Data Protection Regulation 2016/679 (GDPR) and the Spanish Personal Data Protection and Guarantees for Digital Rights Act, which have configured a new regulatory framework on privacy, with a major impact on social media sites. The Spanish Personal Data Protection and Guarantees for Digital Rights Act has added new digital rights that are especially relevant in relation to social media, such as:

- the right to secure data transmission, which will require providers of internet services to be fully transparent when informing their users about the measures they are applying in order to guarantee that right;
- the right to rectification on the internet, which requires a response from online news and media sources when requests for corrections are submitted to them, along with publication of clarification notices in their digital archives if needed in order to explain that their original news story did not reflect an individual's current situation;
- the right to be forgotten on social networks, which involves the right possessed by individuals to have their own personal data deleted if it has been provided by third parties for publication by social network services, whenever such information is inappropriate, inaccurate, irrelevant, outdated, or excessive, or when it has become so, based on the passage of time;
- the right to portability for social network services and equivalent services, which makes it possible for users to retrieve and transfer the contents they have submitted to providers of such services, or to have those contents transferred directly to a third party designated by the user whenever it is technically possible to do so.

Also, in relation to privacy, the European Commission is now working on an e-privacy regulation, that is expected to have a very significant impact on social media.

It is worth mentioning that in April of 2018 the Spanish Legislative Royal Decree 1/1996 of 12 April, which approves the consolidated text of the Spanish Intellectual Property Act was amended (*Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual*). The purpose of these amendments was to standardise, clarify, and harmonise the legal provisions in force on that subject, including amends affecting social media sites, which were added in relation to collection rights for the 'private copying levy', among other issues.

Spain also has specific legislation related to electronic communications and e-commerce, which establishes some rules that affect not only privacy, but also the business practices and initiatives of social media sites. Finally, there is debate now taking place in Spain regarding specific regulation of commercial activities, such as those carried out by YouTubers or advertising targeted at minors and presented via digital media.

Currently, the most severe penalties that can be imposed in relation to social media sites are those involving data protection, with the maximum amount of those fines being EUR20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is greater.

2.10 Review of Industry Participants by Parties Other Than Regulators

In general, there are associations that monitor legislative initiatives and regulatory changes, which help to detect any impacts on each of the areas in which they specialise. In the finance area, the most active associations are the Association of Spanish Banks (*Asociación Española de Banca*, AEB), the Association of Collective Investment Vehicles and Pension Funds (*Asociación de Instituciones de Inversión Colectiva y Fondos de Pensiones*, INVERCO), and the Insurance Business Association (*Unión Española de Entidades Aseguradoras y Reaseguradoras*, UNESPA).

The Spanish FinTech and InsurTech Association was founded in 2016; this was followed in 2018 by the creation of the Spanish Association of Tokens and ICOs (*Asociación Española de Tokens e ICOS*, AETOK), which has FinReg as one of its founding members, as well as Alastria.

Although changes to the law do not always lead to changes in market practices, the legislation on financial markets (eg, MiFID II or PSD2), is showing an increasing influence on the business models adopted by financial institutions.

2.11 Conjunction of Unregulated and Regulated Products and Services

The offering of unregulated products and services in conjunction with regulated products and services is happening in some verticals. Some examples include payment processors that also offer loans as an accessory activity, or aggregators (principal service) that offer initiation services as an accessory activity. Except in the case of some specific licences (such as those for managing collective investment vehicles), the regulators are allowing both regulated and unregulated services to be jointly provided, and in general there is no need to form a separate legal entity in order to do this. In such cases a licence is required for purposes of providing the regulated service, while to offer the accessory service the regulator requires a certain degree of independence or separation between the principal service and the accessory service. The purpose of this requirement is to ensure that the non-regulated activity does not contaminate the regulated activity, which could put the regulated service at risk.

3. Robo-advisers

3.1 Requirement for Different Business Models

The business model for a robo-adviser does not depend upon the type of financial instrument, but rather on other factors such as the type of service being offered (only investment advice or also reception and transmission of orders, and execution of orders – or both – or also custody, etc), the segment of the public towards which the services are being addressed, or the investment alternatives being offered. For example, with the implementation of MiFID II into Span-

ish law, marketing of complex financial instruments to retail clients is prohibited in cases where their terms state that they are intended for professional clients or eligible counterparties, including where such products are bought and sold via a trading venue.

3.2 Legacy Players' Implementation of Solutions Introduced by Robo-advisers

The introduction of robo-advisers in Spain is taking place slowly, and the number of robo-advisers is still small. It must be remembered that in Spain the industry is highly bank-oriented, especially in the field of investments. This means that traditional customers are hesitant to put their trust in a purely online adviser where decisions are taken largely via the use of algorithms. Of course, this tendency will certainly evolve as new generations begin to use such services, since they are already very familiar with online banking and with using apps to manage their finances. It is therefore likely that this barrier to entry now being faced by robo-advisers in Spain will be eliminated.

In fact, some of the traditional banks with the largest volume of assets of retail clients – Openbank, CaixaBank and BBVA, or others such as Bankinter – have recently launched their own robo-advisers, and it is likely that some additional Spanish banks will offer them too, with the trend continuing to spread to other banks as well.

3.3 Issues Relating to Best Execution of Customer Trades

Typically robo-advisers only offer advice on the subject of investment; in other words, although they issue personalised recommendations for clients on the purchase or sale of financial instruments that are suitable for them, they do not typically execute the orders. Therefore, there are no problems of best execution, since there is no direct order from the client. On the other hand, where services are in fact incorporated for receiving, transmitting, and executing orders (or for all of these), the requirements on best execution will apply. As stated in the response to the first question, offering regulated services in addition to providing investment advice has a high impact on the obligations that robo-advisers must face, such as those involving infrastructure, licensing and the information that must be provided to clients.

4. Online Lenders

4.1 Differences in the Business or Regulation of Loans Provided to Different Entities

During the last few years the granting of loans has changed exponentially with the entry of new players into the financial sector. FinTech entities have made the access of individuals and companies to financing more dynamic. In this sense, lending and microlending businesses have been developed, and they have been able to configure their business models

under softer regulatory conditions. It must also be pointed out that in Spain, if loans (including quick loans for very small amounts) are being granted against an entity's own capital, there is no requirement to maintain a reserve for financing activities, and such lending can therefore take place without licensing. This means that there are low regulatory barriers to entry in terms of putting these business models into operation.

Development of microlending initiatives has been focused on offering access to credit for customers considered as sub-prime. This is because traditional credit institutions have been obligated to first perform a significant amount of solvency analysis, and they therefore could not grant access to credit with the same freedom enjoyed by the new FinTechs in the mini-loan segment. In this context, new FinTech entities dedicated to granting loans have focused their efforts in recent years on developing mechanisms that use algorithms to analyse the solvency of loan applicants, backed up by the application of big data techniques.

Based upon this approach, analysis of personal data has become the basis for assessing solvency and debt capacity, through increasingly digital and automated procedures.

This novel situation has been made possible thanks to application of new regulations on personal data protection and also by PSD2. As such, transposition of the PSD2 directive into Spanish law by means of Legislative Royal Decree 19/2018 of 23 November on payment services and other urgent measures on finance, produced new regulations on the ability to access payment accounts for the purpose of aggregating financial information on individuals and performing solvency analysis. On the other hand, the GDPR established the rules for the lawful processing of personal data when automated decisions are being adopted based on analysis of personal data. This new regulatory framework has provided the legal certainty for application of the big data practice applied to the development of new FinTech companies in the credit industry. Meanwhile, traditional loan-granting activities have maintained their primacy in terms of the volume of credit granted on the market, while also taking advantage of new possibilities presented by analytics technologies and its regulation.

Moreover, data protection issues must be highlighted, given the need to evaluate an applicant's solvency prior to granting of a loan – indeed, there is an obligation to do so, depending on the type of entity. In relation to this, companies dedicated to extending credit are carrying out operations where they exchange information with financial solvency databases, engaging in both querying and reporting personal data. Consultation of this type of databases requires compliance with the duty to inform the customers, while reporting debt-related information to those systems requires compliance with Section 20 of the Spanish Personal Data Protec-

tion and Guarantees for Digital Rights Act that requires the information being reported to be accurate, related to debts that have been due-and-payable for no more than five years, and related to debts for which the existence or amount has not been claimed. Furthermore, a formal payment request must be made before any information reported. Adequate consultation is essential in relation to processes of this type, because they are the cause behind many of the auditing and sanctioning procedures initiated by the Spanish Data Protection Agency against entities in the financial sector.

4.2 Underwriting Processes

There is no specific regulation related to underwriting processes in Spain. However, lenders must comply with the requirements defined in:

- Spanish Law 16/2011 on consumer credit agreements, which applies to loans over EUR200, and that includes the rights and obligations of the lender and the borrower (including the rights to withdrawal and early repayment);
- Spanish Law 22/2007 on the distance marketing of financial services to consumers, which establishes the information that credit applicants must receive both before and after requesting financing from a private lender acting on a non-face-to-face environment (eg, operating via the internet).

4.3 Sources of Funds for Loans

In Spain there has been an increase in activities carried out by collective financing platforms (crowdlending), as well as by entities offering quick loans.

Although loans granted using an entity's own capital remain unregulated, Spanish law allows persons dedicated to granting loans on a professional basis to do so as entities that are either regulated (credit institutions or financial credit establishments) or unregulated (companies). In both cases, such entities are subject to the legislation on consumer protection in addition to the Spanish Law of 23 July 1908 on usury, in addition to the cross-cutting AML & CTF and data protection laws. Moreover, if the service is being provided via a regulated entity, that entity will be subject to its own specifically applicable legislation as well. However, even if entities are unregulated the local laws may still introduce specific requirements, such as an obligation to hold civil liability insurance or to be registered with the public registries maintained by consumer protection authorities.

In this area, the biggest problem that arises is the lack of a legal definition regarding the interest rates that should be considered as usurious. That absence of a definition, however, is supplemented by the case law issued by Spain's courts on the subject.

On the other hand, in Spain we have also been seeing a significant increase in collective financing (crowdlending).

According to data from a 2017 annual report on Collective Financing produced in collaboration with the Complutense University of Madrid, during that year the total amount loaned in such a way exceeded EUR36 million, which represents a 68.86% increase with regard to the figure for 2016. Platforms of that type are regulated under Spanish Law 5/2015 of April 27th on promotion of business financing, that establishes requirements for their authorisation (they must receive a favourable report from the Bank of Spain) and registration (with the CNMV). It also prohibits them from carrying out any activities that are reserved for investment services firms or credit institutions.

4.4 Syndication of Loans

Syndication of loans does not currently exist in Spain.

5. Payment Processors

5.1 Payment Processors' Use of Payment Rails

In Spain payment processors can create or establish new payment rails, since they are not required by law to use the ones that already exist. However, despite the fact that freedom of access is established by the regulatory framework, in practice this is very limited.

6. Fund Administrators

6.1 Regulation of Fund Administrators

Fund administrators are regulated entities and the management they perform is regulated by Directive (EU) 2011/61 on Alternative Investment Fund Managers (AIFMD) and Directive (EU) 2009/65 on the co-ordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS). In Spain these entities must be duly authorised by the National Securities Market Commission (CNMV).

In cases where fund administrators provide investment services they must also comply with certain obligations contained in MiFID II in relation to such services.

6.2 Contractual Terms

Although FinTech is not very well developed in the fund administration industry, some managers working in the context of providing investment services are implementing account aggregation solutions that produce added value for their clients. This allows a client to aggregate information regarding all its accounts at a single entity (including accounts held at third-party institutions), and it also enables the advisory services to be provided in a comprehensive manner. This approach will also contribute to increasing competition among entities, since they will become aware about the financial products a client holds with other institutions.

6.3 Fund Administrators as 'Gatekeepers'

Since managers may gain access to privileged information when buying or selling financial instruments for the portfolio of a collective investment vehicle, they are required to have an alert system that can identify potential market abuses as described in the Regulation (EU) 596/2014 of 16 April 2014 on market abuse (Market Abuse Regulation, MAR).

7. Exchanges and Trading Platforms

7.1 Permissible Trading Platforms

Among other aspects, MiFID II governs regulated markets and multilateral trading facilities and it also defines organised trading facilities (this last group is limited to those trading in bonds, securitised instruments, emission allowances and derivatives).

That legislation also regulates systematic internalisers, which are defined as investment firms that, in an organised, frequent and substantial manner, deal on own account when executing client orders outside of the trading taking place at the exchanges (OTC trades), and it applies transparency rules to them that are similar to those applicable to trading venues. MiFID II modifies the regime applied to those systematic internalisers, which has now become a mandatory system, and it also broadens the range of instruments susceptible to be included for such purposes, to include both fixed-yield and variable-yield securities. The aim is to make bilateral trading of this type more transparent, thereby encouraging the use of trading venues.

That legislation also regulates the obligations imposed upon such providers of electronic access as well as the controls they must apply, making those requirements equivalent for the two types of access included within this category: direct market access (where the access-provider supplies the infrastructure to the client), and sponsored access (where it does not).

7.2 Regulation of Different Asset Classes

In relation to infrastructure, MiFID II does not establish different requirements at the product level, although it does limit the operations of organised trading facilities to fixed-yield instruments, as mentioned in response to the previous question. There are, however, some trading platforms that are identified by asset, such as in the case of FX or cryptocurrency platforms.

Moreover, in the specific case of cryptocurrency platforms, and even though they remain unregulated because the legislation does not vary based on the type of instrument involved, the European regulator has stated that some of the assets being traded on those platforms are comparable to financial instruments. Therefore, the existing laws on financial instruments would apply to some specific assets. This is

a challenge for the European Commission, because although trading in some cryptoassets could or should be subject to regulation, there are obstacles that make it difficult to put this into effect. For example, although in Spain the CNMV has already declared that some tokens must be deemed to be financial instruments, the need for financial instruments to be registered in book entry form for purposes of their trading and subsequent settlement prevents those tokens from being integrated into the existing infrastructures.

7.3 Impact of the Emergence of Cryptocurrency Exchanges

In line with 7.2 Regulation of Different Asset Classes, the arrival of cryptocurrency markets is likely to represent a challenge for regulators, who have already stated that in some cases cryptoassets can be considered as financial instruments or electronic money (thus being subject to the specific legislation in each area such as MiFID II, EMD2 or PSD2). Given this environment of regulatory uncertainty, European regulators have already been warning consumers about the risks posed by trading in assets of this type.

However, the requirements and controls defined in Europe's AML & CTF laws are applicable to providers of exchange services for both virtual and fiat currencies, as well as to those providing custody services for them. The applicable regulations establish obligations on transparency due diligence, and it harmonises the requirements that have an impact on those markets.

Finally, in January 2019 the EBA and ESMA published the results of their analysis on application of European law to cryptoassets, and have recommended that the European Commission performs an analysis to define an appropriate response on this subject at the European level.

7.4 Listing Standards

Spanish Royal Decree 1310/2005 of 4 November and Circular 2/2016 establish the requirements that must be met for admission to trading on securities stock exchanges in Spain:

- it must be a publicly traded corporation (Spanish or foreign) with share capital that has been fully paid in, and with no restrictions on share transfer;
- the minimum amount of that share capital is EUR1,202,025 – for determining the existence of that minimum amount, the portion held by shareholders that either directly or indirectly hold an interest of 25% or more must not be taken into account;
- the shares offered must have a minimum market value of EUR6 million;
- the distribution of the shares must be sufficiently broad (as represented in book entry form) to imply that at least 25% are held by members of the public.

Before submitting their request to the CNMV:

- an economic-financial and legal study must be carried out (due diligence),
- their articles of association must be adapted to reflect the status of a publicly traded company (which covers requirements on corporate governance and information and voting rights for shareholders), and
- a corporate website must be created.

Furthermore, companies traded on European regulated markets must produce a prospectus (which must be filed with the relevant authority for review and approval, in the case of the Spain to the CNMV). The information that this prospectus must contain is defined in the EU Delegated Regulation 486/2012. Once this prospectus has been approved it must be published. Once the prospectus is approved the placement phase can begin. The placement is an investment service and it is therefore regulated by MiFID II and by the Spanish Securities Market Act.

In all cases the companies being traded must comply with transparency requirements, both ongoing and occasional. The ongoing requirements most notably include publication each year of the annual accounts, directors' report, and auditor's report, as well as twice-yearly publication of the financial statements or quarterly publication of the partial income statement, among others. The occasional requirements include public disclosure of significant events that could have an appreciable effect on trading of the security, such as payment of dividends, calling of meetings, or changes to board membership, among others.

Right now, we are seeing a higher level of regulation for financial markets, in an effort to ensure the existence of a reliable and transparent market that works in the interest of investors, and with special protection being given to retail participants. In relation to this, most of the principles that the IOSCO published in 2003 on regulation of the securities market are now regulated by European law.

7.5 Order-handling Rules

For investment firms that provide portfolio management services and reception and transmission of orders, MiFID II establishes a duty to act in the best interest of the client. Because of this, those providing investment services must maintain a best-execution policy, which must specify (at the financial instrument level) the entities with which orders are placed or to which they are transmitted for execution. This policy must be made public, and the investment firms must periodically verify the effectiveness of their policy and monitor their execution quality.

However, the legislation also makes it clear that these obligations do not apply when a firm is following specific instructions from its clients.

7.6 Rise of Peer-to-Peer Trading Platforms

See above, 7.2 Regulation of Different Asset Classes and 7.3 Impact of the Emergence of Cryptocurrency Exchanges.

7.7 Issues Relating to Best Execution of Customer Trades

One of the difficulties linked to the obligation to execute orders under conditions that are most beneficial for the client is the need to demonstrate that an entity has complied with this obligation. This implies the need to implement systems that compile market data, price quotes, times, and closing prices.

When instruments are liquid and traded on a regulated market it is relatively easy (although often still costly) to record the prices and demonstrate that trades were executed in a reasonable amount of time or at market price. However, when an instrument is being traded under circumstances of low liquidity or absence of a market (as occurs with some derivatives), with prices being determined according to realities or data that are more unsteady and not reflected on a market, the criteria must be made more objective, and a model or system must be implemented that will allow the data used to demonstrate best execution or fairness of the price to be saved.

Finally, it remains to be seen how the regulator will be able to enforce the best-execution requirement for platforms trading tokens that are considered as financial instruments, or how those platforms must be adapted to comply with the legal requirements. In fact, this is the case, not only in terms of best execution, but also in other areas such as investor protection, transparency, and algorithmic trading.

7.8 Rules of Payment for Order Flow

The MiFID II legislation expressly introduces a prohibition against investment firms receiving any remuneration, discounts, or non-monetary benefits for sending their clients' orders to a specific trading or execution venue, unless the requirements applicable to the incentive system or the obligations on conflicts of interest are being complied with.

This prohibition has affected commission arrangements with financial intermediaries, which must now select their trading and execution venue based on a best-execution policy, and in addition to other information, they are now obliged to provide their clients with information on costs and expenses per service and per financial instrument.

This situation is causing business models to become explicitly oriented towards charging the final client.

8. High-frequency and Algorithmic Trading**8.1 Creation and Usage Regulations**

MiFID II establishes the requirements that investment firms must comply with when using algorithmic trading techniques for their trades, regardless of the type of financial instrument involved. That legislation also defines high-frequency trading and establishes additional record-keeping obligations.

8.2 Exchange-like Platform Participants

The obligations that MiFID imposes upon participants are similar to those that it establishes for the markets, but with some differences due to the differing natures of one type of activity or another. Although investment firms can adapt their systems and controls taking into account the nature, scale, and complexity of their own business model, both the markets and the participants must implement formal structures of governance that include a sufficient number of individuals with knowledge of algorithmic trading systems. They must also implement annual controls and assessments to ensure that the specific requirements on algorithmic trading are being complied with.

8.3 Requirement to Register as Market Makers When Functioning in a Principal Capacity

If investment firms use algorithmic trading to act as market-makers, they will have to carry out those market-making activities continuously during a specified proportion of the trading hours at the trading venue involved. They will be required to sign an agreement with the trading venue, and they must implement controls to ensure that they are complying with the obligations derived from that agreement.

In this way, and except under exceptional circumstances, the legislation ensures market liquidity.

8.4 Issues Relating to the Best Execution of Trades

The use of algorithms clearly represents an advance for trading, with benefits that include obtaining better prices and faster execution that reduces costs, and processing the information needed for execution or for taking the most suitable investment decision based on the parameters defined. In the area of best execution, it is worth emphasising that the MiFID II legislation excludes from the definition of algorithm the smart order routers (SORs), which have the aim of using parameters determined in advance to send the same order to multiple markets, in order to achieve the fastest execution at the best price. This means that the applicable controls and other obligations do not extend to covering these SORs, and this represents an effort to encourage their use to ensure the best execution of the orders.

8.5 Regulatory Distinction Between Funds and Dealers

MiFID II establishes limitations on high-frequency algorithmic trading. It does not distinguish between funds and dealers, but it does establish that the entities performing high-frequency trading must be authorised entities. In this way, it ensures that entities using such techniques can be supervised, in order to monitor the use of HFT and prevent it from being used as a tool for price-manipulation.

In this context, though it depends on each particular case, the primary difference between funds and dealers is the different way in which each of those groups uses algorithmic trading. Funds tend to use algorithms designed to manage investment in cases where they are not directly executing the orders. Dealers, on the other hand, tend to use algorithmic trading for market-making and to execute trades, rather than for the execution of a complex investment structure.

8.6 Rules of Payment for Order Flow

The payment for order flow (PFOF) is defined, according to the British FCA, as: “the practice by which an investment firm executes the orders of a client (typically a broker), receiving a commission not only as agent of the client who sends that order, but also of the counterparty against which the order is executed”.

Over the past years, the FCA, which has been the regulator most active on this topic, has expressed the view that this practice could go against the interests of clients, as the investment firm might be tempted to seek counterparties for its client only from those brokers who pay it the most, regardless of whether they really offer the best conditions to their client. Consequently, the MiFID II legislation has expressly introduced a prohibition against investment firms receiving any remuneration, discounts, or non-monetary benefits for sending their clients’ orders to a specific trading or execution venue, unless the requirements applicable to the inducement system or the obligations on conflicts of interest are being complied with. This limitation is impacting the way brokers are currently routing their orders.

9. Financial Research Platforms

9.1 Registration

Currently, there is no specific legislation on registration of financial research platforms.

9.2 Regulation of Unverified Information

In cases involving rumours or false information related to the instruments admitted to trading, the European Regulation on Market Abuse (MAR) would apply. Furthermore, Spain’s criminal code imposes a penalty of six months to two years in prison, or a day-fine calculated for a period of 12 to 24 months, for using inside information to carry

out transactions or issue trading orders that could produce deceptive indications regarding the supply, demand, or pricing for a security or financial instrument. Such penalties are also imposed if such information is used to ensure that a party, either on its own or in collaboration with others, can maintain a dominant position in the market for such securities or instruments for purposes of setting prices at abnormal or artificial levels.

9.3 Conversation Curation

In Spain there is no specific regulation pertaining to such platforms. See above, **9.1 Registration** and **9.2 Regulation of Unverified Information**.

9.4 Platform Providers as ‘Gatekeepers’

There is no specific regulation of those platforms.

10. InsurTech

10.1 Underwriting Processes

In the insurance area, the use of big data and artificial intelligence is a key part of the processes used to sell policies, because those processes must be based on obtaining large amounts of information about the customer signing the policy, but also because that data needs to be interpreted in a way that allows calculation of an amount that fits the customer’s profile while also being competitive. In relation to this, the greatest impact on these automated processes comes from the legislation related to data protection and AML & CTF, in addition to the specific legislation applicable to insurance distribution.

10.2 Treatment of Different Types of Insurance

The EU’s new insurance distribution directive (IDD) imposes different requirements depending on the type of insurance involved. Specifically, it distinguishes between general insurance and insurance with an investment component (insurance-based investment products, IBIPs). Furthermore, within the general insurance category there is differentiation between life and non-life insurance products, with the pre-contractual information document that must be given to customers being different in each case.

There are also cross-selling practices in this area, where customers are offered a product or service together with an insurance product. With selling of that type, an analysis must be performed to determine the applicable legislation, and the information provided to the customer must be adapted accordingly. These practices include, for example, selling of insurance together with an investment product, a mortgage loan, a credit card, etc.

11. RegTech

11.1 Regulation of RegTech Providers

The providers as such are not regulated. However, given the nature of the services that RegTech firms provide, they must ensure that their technological solution allows the entities contracting their services to comply with their obligations.

11.2 Contractual Terms to Assure Performance and Accuracy

In cases where delegation exists, the company must ensure that the provider can be supervised by the competent authority and that all the information needed in order to allow effective supervision is being provided. It is also important to point out that liability cannot be delegated. It always remains with the service-provider, even in cases where functions can be delegated to a third party.

11.3 RegTech Providers as ‘Gatekeepers’

RegTech providers do not act as ‘gatekeepers’ in cases where they are only providing the technological solution that is enabling a regulated entity (electronic money institution or investment services firm) to comply with its regulatory obligations. In addition, under Spanish law entities that are delegating identification of their customers to comply with AML & CTF legislation can only do so to another entity that is subject to those laws. However, for these purposes they are also allowed to make use of specific technologies that allow such identification to be performed, such as biometric, and there is currently a great expansion in this area.

12. Blockchain

12.1 Use of Blockchain in the Financial Services Industry

In Spain, market participants and their infrastructures are participating in implementation of blockchain technology at a variety of levels, depending on the area that affects them within the financial sector. Many entities, especially those involved with post-trade services and payments, have developed their own innovation laboratories, where they are now testing this technology based upon their own concept-testing. Also, national initiatives such as FTL and Niuron have now come into existence, and they are allowing collaborative work to take place among all participants in the sector.

There is also an initiative known as Alastria. This is a consortium made up of companies and institutions, which has been created in order to establish a semi-public blockchain/DLT infrastructure. The objective is to provide support to services by using blockchain technology in the manner prescribed by law, so that products and services can be distributed in the Spanish market in an efficient manner. The consortium is therefore building the blockchain platform known as Alastria and its libraries, which are made available to the associ-

ated members. These members are then free to make use of the system to carry out their own pilot projects. Those associated with this network include important participants in the finance industry such as *Bolsas y Mercados Españoles* (BME) and the Official Credit Institute (ICO), as well as major banks such as Banco Santander, BBVA, Bankia, and Banco de Sabadell. There are also large non-financial corporations involved such as Iberdrola and Repsol, along with smaller enterprises, insurance companies, payment institutions, universities, etc. Finally, there are some large Spanish entities participating in international consortiums that are focused on new business models as well as on technological standardisation (R3, we.trade, Enterprise Ethereum Alliance, etc).

12.2 Local Regulators’ Approach to Blockchain

In Spain, the CNMV’s plan for 2018 included actions to promote projects related to FinTech and InsurTech, as well as actions meant to address relevant aspects related to blockchain technology and its application to the securities market.

Moreover, in order to define its criteria related to cryptocurrencies and ICOs (see above section 7. **Exchanges and Trading Platforms**), the CNMV created a specific portal at its website used to solve questions and to publish its Q&A documents. It is worth pointing out that as of 30 September 2018, the CNMV had received 235 queries related to FinTech and InsurTech, with 51 of these pertaining to blockchain technology and cryptoassets.

It is also important to mention that the CNMV participated along with BME and various banks (including three from Spain) in a project known as Fast Track Listing (FTL), which is using blockchain technology. That collaborative project has carried out concept testing in relation to registration of a warrant issue. That testing was successful, and it also reduced the time-periods by more than 70%, with the process performed in 48 hours.

Finally, in July of 2018 Spain’s Ministry of the Economy and Business published draft legislation on measures related to the digital transformation. The purpose of this law will be to guide and oversee the innovation process in order to eliminate obstacles to it, while at the same time preserving the principles mentioned. The law will provide for a regulatory sandbox to serve as a testing environment, which is expected to go into operation in 2019.

12.3 Classification of Blockchain Assets

Not all assets based on blockchain technology are considered to be financial instruments. To add to 7.3 **Impact of the Emergence of Cryptocurrency Exchanges**, there are other assets such as those known as ‘utility tokens’ that consist of pre-purchasing of an asset. These cannot be considered as financial instruments, although they are subject to the cross-cutting AML & CTF and data protection laws. However, the

assets known as 'security tokens' are being developed as a type of alternative investment that uses a blockchain to represent a company's stock or other assets. This implies that they would be subject to the applicable legislation in relation to their issuance and subsequent trading on a secondary market, because they are deemed to be financial instruments.

Along these same lines, and in relation to cryptoassets that can be considered as electronic money, the EBA has already stated in a report from January 2019 that a crypto-asset will only be considered as electronic money if it complies with all the elements from the definition found in Section 2.2 of EMD2. There could, therefore, be cases where a crypto-asset, based upon its characteristics, can be considered as electronic money, and it will therefore fall within the scope of applicability of EMD2. In such cases, and in conformity with Title II of EMD2, an entity will need to be authorised as an electronic money institution in order to carry out activities related to electronic money, unless a limited network exemption applies according to Section 9 of that directive. However, since cryptoassets are not banknotes, coins, or scriptural money, they do not fit the definition of 'funds' found in Section 4.25 of PSD2, unless they can be considered as 'electronic money' for purposes of EMD2. In cases where a company is providing any of the payment services included in Annex I of PSD2 using a crypto-asset that can be classified as electronic money, that activity would fall within the scope of applicability of PSD2. That EBA report states that, according to the European Union's current regulatory framework on financial services, cryptoassets may be considered, depending on their characteristics, as financial instruments, electronic money, or neither.

Furthermore, in the Recommendations issued by the FATF in November 2018, changes were adopted in relation to activities that involve what is referred to in their terminology as cryptoassets, with the purpose of clarifying how AML & CTF measures should be applied to certain activities involving virtual assets.

For the time being there have not been any changes to the currently applicable regulation. However, the EBA has asked the European Commission to analyse whether a legislative response is required at the EU level on cryptoassets. It has also requested an assessment of the latest recommendations and any other standards or guidelines issued by the FATF, along with adoption of measures that will, to the extent possible, produce consistency in the way cryptoassets are handled in terms of accounting.

12.4 Regulation of 'Issuers' of Blockchain Assets

There is no specific regulation of issuers of blockchain assets. However, in relation to this the European regulator ESMA has published an advice document on cryptoassets and ICOs, which it explains the mandate issued by the European Commission to European authorities to analyse the alternatives

available for adapting the regulatory framework to assets of that type, and to form a consensus regarding application of the anti-money laundering laws to the majority of the activities that are incorporating cryptoassets.

In Spain, the CNMV has published its criteria related to ICOs, which include a case-by-case analysis used to determine whether they can be considered as negotiable securities, as well as analysis of the premise that involvement of an authorised entity will not be required in relation to their issuance or custody.

12.5 Regulation of Blockchain Asset-trading Platforms

In line with the other responses in this section, MiFID II would be applicable to any platforms where the cryptoassets involved are considered to be financial instruments. In the same way, the obligations derived from the Market Abuse Regulation (MAR) and the regulations on short selling would be applicable. In relation to this, in its advice document on ICOs and cryptoassets the ESMA analyses the problems that platforms face in terms of compliance with the applicable laws, which include most notably:

- the need for platforms to verify the reputations of their members or participants, to ensure that their level of knowledge and experience is sufficient, and to possess appropriate organisational structures and adequate resources;
- the fact that cryptoassets cannot be categorised as equity instruments or non-equity instruments implies that the transparency requirements would not be applied in the European Union in a homogeneous manner;
- the need for revision of the requirements related to record-keeping and reporting of transactions, as well as revision of the identifiers (ISO, CFI), since these are designed for traditional instruments.

Finally, the ESMA states that there may be a need to clarify the types of services and activities that these platforms can provide, and therefore to clarify the applicable legislation. In relation to this, there are platforms that match up the orders they are executing themselves, so it should be analysed whether or not these platforms can be classified as regulated markets, multilateral trading facilities, organised trading facilities, or investment services firms.

12.6 Regulation of Invested Funds

AIFMD establishes the requirements related to authorisation, organisation, conduct, and transparency for alternative investment fund managers that are managing alternative investment funds in the European Union. As discussed in the advice document published by the ESMA on cryptoassets, many of the national supervisors understand that some cryptoassets could be classified as suitable for investment by alternative investment funds. However, the ESMA goes on to

conclude that a deeper analysis must be performed in order to determine the cases in which cryptoassets can fall within the scope of AIFMD, and where they must therefore comply with the obligations established in that directive. In Spain there have not been any specific developments on that issue.

12.7 Virtual Currencies

See above, 7.3 Impact of the Emergence of Cryptocurrency Exchanges.

12.8 Impact of Privacy Regulation on Blockchain

Some experts have warned that a problem arises from the fact that information recorded as chains of data in a blockchain cannot be deleted, but instead can only be rectified or cancelled out through a reference in a subsequent block.

However, it can be argued that the immutability of these data chains should not be considered as an unsolvable problem. Indeed, there are many cases in which the personal data cannot be deleted after being recorded, such as in the records kept at any public registry. Any registry that relies on an interrupted chain of succession and registration to ascertain that the last title or position is a consequence of the first one and the intermediate chain of agreements requires that information logged on the register remains there forever and cannot be deleted.

According to this argument, if we set aside the rules from the GDPR and apply some principles of logic, when anybody accepts the operating rules for a system in order to benefit from it, that party waives any rights that may be incompatible with that system. This situation cannot be considered as representing a restriction of those rights, but rather as a voluntary, legally permissible act of waiver.

However, that party must be aware of the characteristics of the system and the relevance of that voluntary act being performed (the principle of transparency). In addition, the system should never be abusive, and there cannot be any uncertainties regarding the scope of the rights the subject waives.

In other words, before anybody starts carrying out transactions that use a blockchain, that person must be aware of the characteristics and limitations that condition that transaction, and understand and accept that the details related to his or her participation in the chain of events cannot disappear in the future. The use of the chain itself must also be reasonable and proportional in terms of its purposes and operativity. If the party involved accepts all this, then there should not be any problems. The party involved is simply waiving the right to erasure and the right to oppose processing.

For this reason, although the GDPR makes no reference to systems like blockchains, this lack of explicit reference and

rules cannot be understood as impeding the regulation being applied to such systems.

Section 17 of the GDPR establishes that the right to erasure is subject to certain conditions, ordering the data to be erased when the following occurs.

- *The data is no longer needed:* this never happens in the case of a blockchain, because the integrity and immutability of the data chain is what provides certainty for the information and the legitimacy presented by the chain itself. In other words, if the chain is modified it is no longer possible to verify the accuracy and integrity of the information, or the validity of the ownership being confirmed by use of that chain.
- *The data subject has revoked his or her consent or is opposed to the processing, unless any other legal basis applies:* the GDPR guarantees the data subjects' right to revoke their consent and oppose processing of their personal data. However, this right is not absolute. If there is some other legal basis for that data processing, then the right to revoke consent and to oppose the data processing is overridden while that other legal basis for the processing remains. Blockchain relies on a permanent legal basis, which is the other participants' legitimate interest in ensuring that the system remains in operation. If at the time when they decide to participate in the system the participants are aware of the fact that logging their data in the blockchain cannot be reversed, since verification of all subsequent blocks depend upon its presence, their only option is to accept that they cannot request erasure of their data or oppose its processing, because their data will be serving that purpose of subsequent verification. In such cases, the legitimate interest of the other participants in the system, and of the system itself, must be preferent to the interest of the participant that is opposed to the data processing (based on "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject" according to the terminology used in Section 21.1 of the GDPR).

There are also cases where erasure of such data is guaranteed: these are cases where the processing does not have a legal basis, or under circumstances where the law requires such erasure. In such cases, enforcement of the law infringed or the law that establishes the relevant prohibition will require the destruction of the chain itself.

What is certain is that the decentralised structure of a blockchain system will make it very difficult to apply laws that prohibit the business executed via the chain, or that have been violated by the blockchain system itself. Of course, these difficulties are not being generated by the GDPR but rather by the technology, so it would be inappropriate to think that such difficulties are related to Europe's legislation.

In terms of transparency, the blockchain system, like any other data processing system, is subject to the principles of transparency and the duty to inform, as regulated under sections 12, 13, 14, and 15 of the GDPR. There is nothing preventing a person who proposes that someone else carry out legitimate business using blockchain technology from informing them about all the points that GDPR requires. As use of blockchain becomes more regular, this will raise tools to meet this obligation.

Finally, it must be pointed out that the system's decentralisation and dispersal also bring up difficulties in terms of ensuring compliance with the GDPR principles outside the European Union. However, these difficulties cannot impede this technology from being used.

In conclusion, blockchain technology is ideal for digitalising record-keeping systems that rely on traceability, where each act recorded depends on the one recorded before it.

However, we have also seen some initiatives involving application of blockchain technology to systems where traceability is not the aim. In these cases, this technology is inappropriate because its immutability is excessive, and it goes far beyond what is needed. The results pursued could be achieved in a much simpler way.

It may be argued that criticisms of this technology, and the conclusion that it violates right to data protection, refer more to cases of inappropriate implementation of blockchain, where the impediments to the right of data erasure and opposition to processing make no sense.

13. Open Banking

13.1 Regulation of Open Banking

Entry into force of PSD2 has been the spark that has allowed the initiation of open banking in Spain. As such, this new legislation and the obligations it brings with it for banks have provided the stimulus needed to allow authorised third parties to gain access to customer data (especially entities in the FinTech area), and to promote greater competition in the industry. All of this leads to the achievement of PSD2 goals: giving customers more transparency and more control over their banking information.

13.2 Concerns Raised by Open Banking

PSD2 has represented a radical change in the financial services sector, by legitimising and regulating the payment accounts information services and the payments initiation.

Not only has this directive helped to normalise such services, but in practice it aims to decentralise payments-related services, and also encourage competition between financial institutions and new operators in the commercialisation of financial and insurance services.

In this new scenario, these new competitors started to develop innovative marketing systems for banking and insurance products, as well as value-added services based on payment accounts information analysis.

In this situation all players, including both traditional banks and new FinTech firms, have started to give personal information a new value that was never considered up until now, since the new competitor's main strength is its ability to engage in personalised selling and the individualisation of products.

The GDPR has also established a regulatory framework that allows further development of activities based on big data and information analysis by clearly establishing the principles that allow for the application of (and the granularity of) the purposes of data processing – therefore, entities have had to adapt the conditions that governs their data processing, clearly differentiating the processing of data authorised by the need to comply with contractual terms from the processing of data governed by consent or carried out by virtue of a legitimate interest. This has required them to inform their customers or users regarding the purposes behind analysis of their personal information, stating the specific aims being pursued and identifying the legal basis that supports the processing.

In the end, entry of the GDPR into force and application of PSD2 have allowed the coexistence of two types of radically different entities, the traditional banks and the new operators, and has provoked competition between them for the benefit of consumers. The new regulatory framework has been a catalyst for technological innovation. All the entities that are competing in the market designed by PSD2 are looking for personal data analysis-based solutions, in order to increase their competitiveness and improve the clients and customers treatment.

In this sense, entities competing in the financial and insurance products market have been able to ensure their compliance with the principles of transparency and legitimacy of data processing, before developing new marketing plans for those products.

finReg360

C/ Alcalá, 85,
28009 Madrid

Tel: +34 910 496 459
Email: info@finreg360.com
Web: www.finreg360.com



In terms of security, and given the enormous value that personal information has acquired – based on its ability to be analysed – entities are also investing in the protection of that information from a technological perspective, revising the structure of their IT systems and looking for tools and solutions that will help them to ensure that no weaknesses that could put that information at risk exists.