INFORMATION GUIDE FOR APPLICANTS FOR AUTHORISATION OF PAYMENT INSTITUTIONS OR ELECTRONIC MONEY INSTITUTIONS, AND FOR REGISTRATION OF NATURAL OR LEGAL PERSONS PROVIDING ACCOUNT INFORMATION SERVICES OR EXEMPT ACCORDING TO ARTICLE 14 OF ROYAL DECREE-LAW 19/2018

[Note: This document is a translation of the document named *"Guía informativa para solicitantes de autorización de entidades de pago o de entidades de dinero electrónico, así como de registro de personas físicas o jurídicas prestadoras del servicio de información sobre cuentas o exentas a las que se refiere el artículo 14 del real decreto-ley 19/2018".* **In case of discrepancy, the Spanish version shall prevail.**]

1 GENERAL ASPECTS OF THE PROCEDURE

This information guide is drafted in accordance with the provisions of Article 2.5 of Royal Decree 736/2019 of 20 December on the legal regime for payment services and payment institutions, and Article 2.2 of Royal Decree 778/2012 of 4 May on the legal regime for electronic money institutions (the "**Guide**"), and shall be applicable to the actions carried out by the Banco de España in the exercise of the following procedures:

- Authorisation of payment institutions and electronic money institutions
- Registration of natural or legal persons providing account information services
- Registration of natural or legal persons exempt from the legal regime applicable to payment institutions referred to in Article 14 of Royal Decree Law 19/2018

The purpose of this Guide is to inform applicants for authorisation or registration for the provision of payment or electronic money services (the "**Applicants**"), of the formalities, requirements and criteria applied in the above-mentioned authorisation or registration procedures (the "**Authorisation or Registration Procedures**"), and it must be read along with the forms referred to in Section 1.5 of this Guide, which complement it.

Hereinafter, any mention of "**Institution**" shall be understood as made to the natural or legal person for which the Applicant requests authorisation or registration in accordance with the provisions herein (which, in certain cases, shall coincide with the Applicant).

The Guide will be updated whenever necessary to reflect the answers to the questions most frequently raised by the Applicants.

1.1 APPLICABLE LEGISLATION

Authorisation and Registration Procedures shall be governed by the following regulations (although the last two will only apply to authorisation and registration procedures of electronic money institutions):

- Royal Decree-Law 19/2018 of 23 November on payment services and other urgent financial measures ("**RDL 19/2018**").

- Royal-Decree Law 736/2019 of 20 December on the legal regime governing payment services and payment institutions ("**RD 736/2019**").

- Law 21/2011 of 26 July 2011 on electronic money ("**Law 21/2011**")[1].

- Royal Decree-Law 778/2012 of 4 May on the legal regime governing electronic money institutions ("**RD 778/2012**")[2].

In any event, the interpretation and application of these regulations shall be in line with the criteria set by the European institutions and bodies. Thus, any guidelines and recommendations issued by the European Banking Authority ("**EBA**") in accordance with Article 16 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 shall serve as reference.

With regard to the administrative procedure, in all matters not provided for in these regulations, the general rules set out in Law 39/2015 of 1 October 2015 on the Common Administrative Procedure for General Government (**"Law 39/2015"**) shall apply.

In addition, payment or electronic money service providers must comply with the provisions of Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 ("**Regulation 2018/389**") insofar as they may apply to them.

1.2 INTERESTED PARTIES

This Guide is for information and practical purposes. It is aimed at natural or legal persons who intend to provide payment or electronic money services on a professional basis in Spain, under the categories of (i) payment institution, (ii) electronic money institution, (iii) natural or legal person providing account information services, or (iv) natural or legal person exempt from the legal regime applicable to the payment institutions as referred to in Article 14 of Royal Decree-Law 19/2018, and that, therefore, must apply to the Banco de España for authorisation or registration, as well as to those persons seeking to ascertain whether the activities they wish to carry out are subject to any of these procedures, and what requirements they would have to meet in order to apply for the relevant authorisation or registration.

Some of the examples of business models that, in principle, should request authorisation or registration under the terms detailed here are companies other than credit institutions that, solely or in addition to other economic activities: provide money transfer services (remittance operators); offer payment or electronic money accounts that allow for payments to be made and received; issue credit or debit or prepaid cards; engage in the acceptance

[1] As amended by RDL 19/2018.

[2] As amended by RD 736/2019.

and processing of transactions at businesses with debit and credit or prepaid cards; aggregate account information or initiate payment transactions.

Lastly, with regard to financial credit institutions that wish to apply for authorisation to also provide payment or electronic money services, these provisions will also apply, although the specificities applicable to this type of institution by virtue of the regulations applicable to them should be taken into account.

1.3 BEFORE INITIATING THE PROCEDURE

The envisaged duration for processing Authorisation or Registration Procedures tends to be extended, either because the programme of operations or the business plan are not sufficiently detailed, or because the documentation submitted is not complete, or does not allow for verification of compliance with the requirements set out in the applicable regulations. Therefore, before formally submitting the application, the business model to be implemented must be defined precisely and the Applicant must be familiar with the applicable regulations and with the documents to be submitted.

In addition, Applicants are offered the possibility of holding a meeting prior to formally submitting the application, in order to discuss the most salient features of the project and to resolve doubts about the procedure. To arrange the meeting, Applicants must submit the pre-application form found at the "Tramitación" section within the corresponding authorisation or registration procedure of the Banco de España's Virtual Office duly completed, along with all the documentation indicated therein by Electronic Registry, indicating in the form of presentation by Electronic Registry an email and DNI/NIF/NIE for the purposes of notifications, enabled to access Dirección Electrónica Habilitada Única (DEHú).

1.4 HOW TO INITIATE THE PROCEDURE

The person interested in initiating any of the Authorisation or Registration Procedures must complete the application form available in the "Processing" section of the corresponding procedure at the Banco de España's Virtual Office, and submit it to the Banco de España along with the other forms and documentation referred to in the following section.

The signatory of the application must prove that he/she has sufficient representative powers and that these have not been conditioned or limited, by filing the corresponding deed of power of attorney or appointment, or by any means valid in law which provide authenticated evidence of the representation.

The application for authorisation or registration can be submitted: (i) electronically, through the Banco de España's Electronic Registry, (ii) in person, at the Banco de España's General Registry (calle Alcalá 48, Madrid), (iii) at any of its branches, addressed to Vicesecretaría General – División de Autorizaciones, or (iv) by post, although submission by electronic means is recommended since, in addition to complying with all the security guarantees

established through the use of the digital signature certificate, it guides the Applicant in submitting the application, detailing the documentation that needs to be provided.

The application for authorisation or registration and the processing of the corresponding Authorisation or Registration Procedure are free of charge and no deposit is required.

1.5 REQUIRED DOCUMENTATION

The Banco de España has prepared specific forms for each of the Authorisation and Registration Procedures, based both on the EBA GL/2017/09 Guidelines and on the applicable regulations (as detailed in Section 1.1 of this Guide). These forms are structured in sections identifying the information that must be submitted along with the application and they can be accessed through the links included in the corresponding section of this Guide.

The information provided by the Applicant must be true, accurate and complete. The level of detail must be proportionate to the Institution's size and its internal organization, and to the nature, scope, complexity and riskiness of the particular service(s) to be provided. Likewise, the Applicant may request that any documents already held by the Banco de España be included in the file. In these cases, the Applicant must properly identify the documents to be included and confirm that there have been no changes in the information provided at the time.

The application itself, the legal documentation that must be registered such as the Entity's by-laws, the framework contract to be signed by the users in Spain or the terms and conditions, the customer ombudsman rules or the money laundering prevention manual must be submitted in Spanish, and the remaining documentation may be submitted in English. All this without prejudice to the fact that, at the discretion of the Bank of Spain, the total or partial translation, sworn or not, of certain documents may be required, at different stages of the procedure, based on their relevance.

The application will be deemed to be complete if it contains all the information needed by the Banco de España in order to assess the application, in accordance with the forms and applicable regulations.

Where the information provided in the application is deemed to be incomplete, the Banco de España will send a request to the Applicant or, where applicable, to the person designated for notification purposes,[3] indicating what information is missing and offering them the opportunity to submit it. This request will be sent via the Electronic Notification Service, provided that the Applicant is required or has chosen to communicate with public authorities electronically. Similarly, the Banco de España may request from the Applicant any data, reports or clarifications deemed appropriate for the purpose of assessing the application.

[3] For notifications to be sent to a designated person for notifications purposes other than the promoter, a signed written statement from the latter, either on the application form or in a separate document, must be submitted.

In the event of any change affecting the accuracy of the information and documentation provided in the Authorisation or Registration Procedure, the Banco de España shall be informed without delay.

When new documentation is submitted, either as an update of the information or in response to a request from the Banco de España, the changes made to the previous documentation must be identified in order to facilitate its review.

For further details on the legally established requirements for documentation or information to be provided and the criteria applied to the procedures, please refer to Sections 2 to 4 of this Guide.

1.6 DEPARTMENT IN CHARGE OF PROCESSING THE PROCEDURE

The procedure will be processed by the Authorisations Division, which reports to the Deputy General Secretary of the Banco de España, in collaboration with other Banco de España departments and divisions.

1.7 REPORTS REQUIRED

In the processing of Authorisation and Registration Procedures, when applicable under current regulations, the Banco de España will require reports from:

- The Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences.

- Competent supervisory authorities of the Member States in which the institutions that exercise or will exercise control over the Institution under the terms of Article 42 of the Spanish Commercial Code operate or have operated.

When deemed necessary, reports may also be requested from other bodies such as the National Securities Market Commission, the Directorate General of Insurance and Pension Funds, or any other body.

1.8 DEADLINE FOR DECISIONS ON PROCEDURES AND SUSPENSION OF DEADLINE

The deadline for decisions to be made on the procedures for (i) authorisation of payment institutions, (ii) authorisation of electronic money institutions, and (iii) registration of natural or legal persons providing account information services, is three months from the receipt of the application if it is complete, or from the moment the necessary documentation is completed. If this period elapses without notification of an express decision on the application, the application shall be deemed denied and the procedure will be terminated.

With regard to the procedure for the registration of natural or legal persons exempt from the legal regime applicable to payment institutions referred to in Article 14 of RDL 19/2018, the deadline for a decision is twenty days from the submission of all documentation referred to

in Article 4 of RD 736/2019. If this period elapses without notification of an express decision on the application, the application shall be deemed successful.

The course of these terms may be suspended:

- When the Applicant is required to correct shortcomings and/or provide documents and other items deemed necessary by the Banco de España, for the period between the notification of the request and its effective compliance by the Applicant, or for the period granted.

- When mandatory reports are requested, for the period between the request and the receipt of the report, but in no case may the suspension exceed three months.

1.9 DECISION

Once the application has been assessed with the documentation provided, the authorisation or registration will be granted or denied.

The authorisation or registration may be denied with indication of the grounds as set out in the applicable regulations, and in any case the Applicant will be given a hearing process before the decision to deny registration is adopted.

If the procedure is deemed successful, certain conditions may be included which must be complied with prior to registration in the Banco de España's Special Registry, as well as obligations or recommendations which the authorised Institution will have to comply with or take into account, as appropriate. In most cases, these are prior commitments that are assumed by the actual Applicant and which are subsequently included in the decision. In no case will these conditions exempt the Applicant from complying with all the requirements necessary for the granting of the authorisation or registration.

The Applicant may formally withdraw its application at any time during the procedure, which will result in the termination of the procedure and the corresponding decision.

Finally, when the procedure is stopped for reasons attributable to the Applicant, the Banco de España will warn the Applicant that it will expire after three months. If this period elapses without the Applicant taking the necessary action to resume the procedure, the Banco de España will agree to shelve the proceedings and notify the Applicant accordingly. The relevant appeals will be permitted against the decision declaring the expiry.

1.10 REGISTRATION IN THE BANCO DE ESPAÑA'S SPECIAL REGISTRY

Once the Applicant has been notified of the granting of the corresponding authorisation and the Institution has been registered, where applicable, in the Mercantile Register, the Applicant will have to apply for registration of the Institution in the Banco de España's Special Registry, subject to compliance with any conditions that may have been imposed for this purpose, submitting alongside the application for registration the corresponding

documentation as indicated in the Virtual Office. Should the application for registration be defective or incomplete, the Applicant shall be required in writing to rectify it within the deadlines established from time to time.

The Institution may not commence its activities until it is registered in the Banco de España's Special Registry.

It is a condition for such registration that there be no substantial changes to the terms on which authorisation has been granted. As indicated in section 1.5 of this Guide, any substantial change affecting the accuracy of the information and documents provided in connection with the application for authorisation must be notified to the Banco de España without delay and for the appropriate purposes.
Finally, it should be remembered that failure to use the authorisation or registration within twelve months is one of the causes that could lead to the revocation of the authorisation granted.

2 AUTHORISATION OF PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS

This section applies to those institutions that have their central administration or registered office in Spain and for which authorisation is requested to provide payment or electronic money services on a professional basis in Spain, and which are not exempt or excluded or constitute another type of payment service provider that can provide such services.

Electronic money institutions have the possibility of providing payment services as well as providing the electronic money issuance service, both in relation to the electronic money they issue and in relation to other funds, without the need to be authorised as payment institutions. In any case, the application must include all the payment services to be provided and the authorisation, if any, shall only cover these services.

The authorisation regime for payment institutions is regulated by Article 11 of RDL 19/2018 and the regime for electronic money institutions by Article 4 of Law 21/2011. As regards documentation requirements, Article 2 of RD 736/2019 must be taken into account for payment institutions and Article 2 of RD 778/2012 for electronic money institutions.

The Banco de España has prepared the following forms whose sections identify the information which must accompany the application:

- Payment Institution Authorisation Form
- Electronic Money Institution Authorisation Form

The specific sections of the form are described in detail below, clarifying some of the matters that give rise to questions most frequently.

2.1 IDENTIFICATION DETAILS

The identification details of the Institution for which authorisation is requested must be provided. In particular, it must be confirmed that the registered office and the address of the central administration, as well as its actual management, will be located in Spain.

Likewise, a draft of the by-laws must be provided with the planned amendments to the corporate purpose with tracked changes, in line with the activities that the Institution will carry out once the authorisation is obtained, as well as a certificate indicating availability of the proposed corporate name (not necessary for incorporated institutions that will not change their name).

2.2 PROGRAMME OF OPERATIONS

A report must be provided identifying the type of services envisaged and whether they fall under any of the legal categories of payment services defined in Article 1.2 of RDL 19/2018 and/or the services of issuance, distribution and redemption of electronic money defined in Law 21/2011. A description must be given of how payment transactions are executed, including, inter alia, the procedures for authorising transactions, the settlement arrangements and the processing, settlement and clearing times; a diagram of flow of funds reflecting the transactions must also be provided.

If the Institution is going to provide payment initiation services (Article 1.2(g) of RDL 19/2018) or account information services (Article 1.2(h) of RDL 19/2018), details must be provided on how these services will be provided to users and how the Institution will obtain, manage and use users' credentials and data as well as their consent to such processing.

It must also be confirmed whether, in addition to the provision of payment or electronic money services, the Institution will carry out ancillary activities or other business activities within three years from the authorisation.

If the Institution is to carry out business activities other than payment services or the issuance of electronic money, and the turnover of such business activities is, in the opinion of the Banco de España, significant in terms of risks or profits obtained, it shall have hybrid status. In these cases, the Banco de España may require the Institution to set up a separate institution for the provision of the regulated services if it considers that said business activities could jeopardise the financial soundness of the Institution or create serious difficulties for exercising supervision.

There must also be a clear indication as to whether the Institution will grant credit in relation to the execution of payment transactions and under what conditions this credit will be granted. The Institution must confirm that it will not be granted with a charge to the funds received in possession for the purpose of executing a payment transaction.

In addition, the draft framework contract to be signed by the users to whom the Institution will provide such services or the conditions of use to which they will have to adhere must

be provided. These contracts must (i) clearly identify the services to be provided to users and under what conditions, (ii) include a reference to the legal nature of the Institution, and (iii) indicate the safeguarding method adopted by the Institution if applicable.

2.3 BUSINESS PLAN

A marketing plan shall be provided as well as a business plan referring to all the activities that the Institution will carry out. The business plan must contain sufficient detail to prove that the Institution will have sufficient financial and other resources that may be necessary to carry out its activity.

Budget forecasts for the Institution's first three financial years of activity must be submitted, including an income statement and a balance sheet, prepared in accordance with Banco de España Circular 5/2020 of 25 November 2020 and using the templates available at the Banco de España's Virtual Office, both for a scenario in which the Institution operates normally and for a stress scenario in which the Institution is expected to incur greater losses.

The business plan must also include details of the main items of the profit and loss account and the balance sheet, and a description of the assumptions on which these items are based. Additionally, if the Institution is already incorporated, it must provide its financial statements (audited if applicable) for the previous three years or a summary of its financial situation if it has not yet drafted its financial statements. The above-mentioned forecasts must be based, where appropriate, on the Institution's situation at the latest available date.

If the Institution is going to carry out business activities other than payment services or the issuance of electronic money, a breakdown must be provided of the contribution of these businesses to the different items of the business plan.

In addition, available and required own funds forecasts for the first three years of the Institution's activity must be provided, for which purpose the definitions relating to this effect in RDL 19/2018, which in turn refers to the solvency regulations for credit institutions, must be taken into account.

The following shall be taken into account in the calculation of the required own funds:

- For electronic money issuance services, the Institution's own funds may not be less than the higher of EUR 350,000 or 2% of the average amount of electronic money in circulation over the previous six months. Electronic money institutions that offer payment services not linked to electronic money issuance services must have additional own funds calculated in accordance with the following point.

- For payment services, the Institution's own funds may not be less than the higher of the initial capital (as described in Section 2.5 of this Guide) and the amount calculated as follows.

The Institution shall communicate which calculation method will be used over the next three years, from among the methods provided for in annex of RD 736/2019 which, in summary, are based on the following:

- Method A: Own funds required shall be, at least, equal to 10% of overhead expenses.

- Method B: Own funds required shall be, at least, equal to the sum of certain items multiplied by the total amount of the payment transactions to be executed.

- Method C: Own funds required shall be, at least, the result of applying a scale factor to certain performance indicators for the year.

Regardless of the method selected, the Institution shall provide the calculations using each of the methods provided.

Additionally, if the Institution is going to grant credit in relation to the payment services envisaged in Article 1.2(d) or (e) of RDL 19/2018, it must provide evidence that it will have adequate own funds taking into account the amount of credit granted.

Available own funds are deemed to be own funds as defined in Article 4.1.118 of Regulation (EU) No 575/2013. For this purpose, own funds shall include those established in Title 1, Part Two of this Regulation, where Tier 1 capital (Common Equity and Additional) and Tier 2 capital are defined, including their eligible items, filters and deductions, insofar as they are applicable. Moreover, Tier 1 capital must be composed of at least 75% of Common Equity Tier 1 capital. Also, Tier 2 capital shall not exceed one third of Tier 1 capital.

2.4 STRUCTURAL ORGANISATION

The Applicant must provide a description of the structural organisation of the Institution, including, where appropriate, a description of the intended use of agents and branches and the off-site and on-site checks that the Institution undertakes to perform, at least annually, as well as a description of the operational outsourcing arrangements and of its participation in a national or international payment system.

The Institution must have an adequate organisational structure and well-defined, transparent and consistent lines of responsibility.

A copy of the main agreements under which the Institution will outsource[4] its operational functions deemed important[5] must be provided, as well as a description of the outsourced

[4] The term outsourcing shall include both the delegation of the performance of operational functions to a third party and any subsequent delegations that the third party may make.
[5] An operational function will be deemed "important" if an anomaly or shortcoming in its execution may substantially affect the Institution's capacity to permanently meet the conditions arising from its authorisation, or its other obligations under the regulatory framework applicable to it, or affect the financial results, soundness or continuity of its regulated services and the confidentiality of the information it handles.

activities, the identity and geographical location of the outsourced service provider, the internal controls and the persons within the Institution who will be responsible for each of the outsourced activities. Such agreements must include a clause providing for direct and unrestricted access by the Institution and the Banco de España to the Institution's information held by the third parties, and the possibility of verifying, on the third parties' own premises, the suitability of the systems, tools and applications used in the provision of outsourced functions. The governance framework of the outsourcing agreements shall also be assessed, indicating the risk analysis methodology and scope, including for risks arising from the location of the third parties, and the business continuity plans in the event of termination of the outsourcing and the controls to be carried out on the outsourced activity.

The outsourcing of these important functions must not lead to a complete emptying of the content of the Institution's general activity.

Lastly, a list of all natural or legal persons that will have close links[6] with the Institution must be provided, indicating their identity and the nature of those links. Such close links must not hinder the effective exercise of supervisory functions or impair the Institution's ability to provide timely and accurate information to the competent authorities.

2.5 EVIDENCE OF INITIAL CAPITAL

Documentation must be provided as evidence that the Institution has or will have at the time of its authorisation the initial capital required: (i) EUR 20,000 if the Institution will only provide money remittance; (ii) EUR 50,000 if the Institution will only provide payment initiation services; (iii) EUR 125,000 if the Institution is going to provide any of the services referred to in Article 1.2(a) to (e) of RDL 19/2018, regardless of whether or not it will provide other payment services; or (iv) EUR 350,000 if the Institution is going to provide electronic money services, regardless of whether or not it will provide payment services, whether they are linked to the issuance of electronic money or otherwise.

If the Institution is incorporated, the Applicant must provide its financial statements to prove that the Institution has the initial capital required. If, on the other hand, it is not incorporated, or if it is incorporated and its financial statements do not show that the Institution currently has the initial capital required, it must prove that it has the initial capital required by providing a bank statement issued by a bank certifying that the funds are deposited in a bank account owned by the Institution.

This initial capital must be accredited without prejudice to the fact that the Institution must comply with the share capital or other items, in accordance with the provisions of other specific regulations applicable to it.

It must be noted that the initial capital is not equivalent to share capital, but rather it includes the following items: (i) equity instruments, (ii) share premium accounts, (iii) retained earnings,

[6] "Close links" means a situation in which two or more natural or legal persons are linked in any of the following ways: (i) participation in the form of ownership, direct or by way of control, of 20% or more of the voting rights or capital of an undertaking; (ii) control; or (iii) a permanent link of both or all of them to the same third person by a control relationship.

(iv) accumulated other comprehensive income, or (v) other reserves, in accordance with Article 26.1(a) to (e) of Regulation (EU) No. 575/2013.

2.6 MEASURES TO SAFEGUARD USERS' FUNDS

A description must be provided, indicating which of the following procedures will be adopted by the Institution to safeguard funds received from users of payment services or electronic money issuance services or through other payment services providers for the execution of payment transactions:

- Segregation at all times and their (i) deposit, if still held by the Institution at the end of the working day following its receipt, in a credit institution subject to prudential supervision and domiciled in a European Union Member State, which holds balances in favour of customers, or (ii) subsequent investment, if still held by the Institution at the end of the working day following its receipt, in safe, liquid and low-risk assets (assets which have a zero credit risk weighting in accordance with banking regulations).

- Insurance policy or other comparable guarantee from an insurance company or a credit institution authorised to provide services in Spain and which does not belong to the same group as the Institution. The guarantee or insurance policy must be direct and on first demand, cover all users' funds and not contain any clause the fulfilment of which is outside the direct control of the Institution and which allows the provider of the guarantee or insurance policy to unilaterally cancel or reduce the term of the guarantee or insurance policy.

A draft copy of the contract to be signed by the Institution regulating the selected procedure must be provided. If the funds are to be safeguarded by being deposited in a credit institution, the draft contract must (i) make express mention of their condition as "payment institution customer balances" or "electronic money institution customer balances", as appropriate, (ii) exclude any clauses which lead or may lead to mistaking them with the funds of natural or legal persons who are not payment service users on whose behalf the funds are held, such as those arising from netting or the debiting of fees, and (iii) mention the absolute right of segregation of accounts and assets, with respect to possible claims of other creditors, in the event of the Institution's insolvency.

It shall not be necessary to complete this section if the Institution is only going to provide (i) payment initiation services by itself, or (ii) payment initiation service together with account information services.

2.7 CORPORATE GOVERNANCE PROCEDURES AND INTERNAL CONTROL MECHANISMS

The Applicant must provide a description of the Institution's corporate governance methods and internal control mechanisms, including administrative, risk management and accounting procedures, demonstrating that they are proportionate, appropriate, robust and adequate.

Also, as evidence of safeguarding, corporate governance methods and internal control mechanisms, security incidents and structural organisation, the Applicant must provide a description of the Institution's audit procedures and the organisational arrangements to be put in place in order to take all reasonable steps to protect its users' interests and to ensure the continuity and reliability of the issuance of electronic money and/or the provision of payment services.

2.8 PROCEDURE FOR MONITORING, HANDLING AND FOLLOWING UP ON SECURITY INCIDENTS AND SECURITY-RELATED CUSTOMER COMPLAINTS

A description must be provided of the procedure in place to monitor, handle, follow up on and resolve security incidents and security-related user complaints, including an incident reporting mechanism that meets the Institution's reporting obligations as set out in Article 67 of RDL 19/2018. This description shall include:

- The measures to be adopted for fraud prevention, both at the organisational level (e.g. implementation of the three lines of defence or regular review of records) and the tools used for this purpose (e.g. tools for generating, auditing and reviewing records, etc.).

- Details of the persons and bodies responsible for providing assistance to customers in the event of fraud, technical incidents and/or handling claims and complaints, indicating the point of contact.

- The reporting lines in the event of fraud, including the possible channels for receiving fraud-related incidents, cooperation between teams, departments and/or providers, along with their escalation within the Institution.

- The procedures for reporting incidents, including their communication to internal or external bodies, and for reporting serious incidents to the national competent authorities, in accordance with Article 67 of RDL 19/2018. For these purposes, it is recommended to take as reference the procedure available in the Banco de España's Virtual Office, aligned with the criteria set out in the EBA/GL/2017/10 Guidelines, which will be replaced, effective from 1 January 2022, by the EBA/GL/2021/03 Guidelines.

- The supervision tools used and the monitoring measures and procedures adopted to mitigate security risks, beyond those related to fraud prevention.

2.9 PROCESS FOR FILING, MONITORING, TRACKING AND RESTRICTING ACCESS TO SENSITIVE PAYMENT DATA

The Applicant must provide a description of the procedure in place to file, monitor, track and restrict access to sensitive payment data, including:

- All flows in which data classified as sensitive payment data appear, whether at rest or in transit, specifying the actors, systems and data involved.

- The procedures established to authorise temporary or permanent access to sensitive payment data, indicating the persons, roles and/or departments involved in such procedures, along with the different steps in the approval flow and their respective evidence.

- The monitoring tools used (indicating whether developed in-house or by third parties), their main features and how they will contribute to the objective of monitoring access to sensitive payment data.

- The policy on access rights to all relevant infrastructure components and systems, including databases and supporting infrastructure. The list of such components, the roles that have access to them and the type of permission granted (e.g. read, write, etc.). The scope of all the permissions managed in the organisation, including those granted, if any, to certain operations using certain tools. Where they exist, the specific access management tools, detailing their most relevant functionalities and intended use.

- Information on the computer system and technical security measures, encryption and/or tokenisation, including at least the encryption and decryption algorithms used, where the keys will be stored, their backup and who or which roles will have access to such keys.

- An explanation of how breaches are to be detected and dealt with, bearing in mind internal breaches, both within the Institution and at its providers, if any.

- The annual internal control programme in relation to IT system security, including the systems involved in sensitive payment data and all systems supporting the organisation, especially those relevant to the provision of payment services.

This description must also include, in all cases, the criterion adopted by the Institution for the classification, in the context of the programme of operations submitted, of data as sensitive payment data, as well as the complete list of the data classified as such under this criterion.

To adopt the aforementioned classification criterion, the Institution shall comply with the definition of sensitive payment data set forth in Article 3.12 of RDL 19/2018, avoiding possible confusion with other terms such as “confidential information” or those relating to the security of personal data, such as “confidential personal data” or “sensitive personal data”.

Furthermore, the description of the technical measures that have been implemented to ensure the security of sensitive payment data should comply with Regulation 2018/389 with

regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

2.10 BUSINESS CONTINUITY ARRANGEMENTS

The Applicant must provide a description of the Institution's business continuity arrangements, clearly defining, in particular, the major operating functions, effective contingency plans and a procedure to test and review periodically the adequacy and efficiency of these plans. This description shall include:

- A business impact analysis including business functions, supporting processes, third parties involved and information assets identified and classified in terms of criticality, along with restore time targets and associated restore point targets.

- Identification of the back-up site or provider, access to IT infrastructure and the key software and data that the Institution would use to recover from a disaster or interruption.

- A description, among other scenarios, of key system failures, loss of key data, loss of access to facilities and loss of key individuals, identifying, at least, the Institution's key persons or roles, their backups and the envisaged procedures for transferring knowledge, taking into account any operational functions that may have been fully or partially outsourced to service providers and describing how continuity of those functions will be managed.

In describing these arrangements, the Institution must take into account the provisions of Section 1.7 "Business Continuity Management" of the ICT and Security Risk Management EBA/GL/2019/04 Guidelines of 28 November 2019.

2.11 THE PRINCIPLES AND DEFINITIONS APPLICABLE TO THE COLLECTION OF STATISTICAL DATA ON PERFORMANCE, TRANSACTIONS AND FRAUD

The Applicant must provide a description of the principles and definitions applicable to the collection of the statistical data on performance, transactions and fraud.

This description must include the submission to the Banco de España of the statistical data on fraud in relation to different means of payment, as referred to in Article 67.4 of RDL 19/2018. In this regard, it must:

- Identify the applicable data breakdown(s) from Annex 2 to the EBA/GL/2018/05 Guidelines of 17 September 2018 on fraud reporting requirements (amended by the EBA/GL/2020/01 Guidelines of 22 January 2020), based on the payment service(s) provided and the payment instrument(s) used.

- Take into account the procedure for reporting fraud data to the Banco de España, available at the Banco de España's Virtual Office.

2.12 SECURITY POLICY DOCUMENT

A security policy document must be provided, including a detailed risk assessment in relation to its services provided and a description of the security control and risk mitigation measures taken to adequately protect the users of these services, including fraud and illegal use of sensitive and personal data. This document shall include:

- The detailed risk assessment of the payment service(s) that the Institution intends to provide, taking into account at least operational and security risks and risks relating to fraud and the outsourcing of operational functions. This assessment includes:
    - an inventory of business functions, supporting processes and information assets classified by criticality;
    - an assessment of the risks associated with the inventoried business functions, supporting processes and assets, taking into account all known threats and vulnerabilities; and
    - a description of the security measures needed to mitigate the operational and security risks identified as a result of the above assessment, indicating those already implemented and those, if any, that are planned to be implemented, along with the timetable established for that purpose.

- A list of all envisaged authorised connections from the outside (including, but not limited to, those relating to the partners, service providers, other group entities and employees) and, for each of these, a description of the logical security measures and mechanisms to be implemented, indicating:
    - whether the envisaged measure is of a technical or organisational nature;
    - whether it is of a preventive or detective nature;
    - whether the envisaged controls entail real-time monitoring or are based on regular reviews;
    - the use, where appropriate, of an active directory that is separate from the group;
    - the management of the opening and closing of communication lines;
    - a description of the security equipment used, whether proprietary or outsourced to service providers (including firewalls, IDS/IPS, system monitoring, antivirus systems, logs/record management systems), indicating the product's trade name or, if self-developed, its main features and how it will be used;
    - whether the use of authentication systems is envisaged, such as those based on key generation or client authentication certificates, together with a description of such systems; and
    - how communication confidentiality will be handled.

  In cases where use is made of a technological infrastructure managed through service providers, such infrastructure shall be considered as the Institution's own and connections to such infrastructure (e.g. connections used by administrators or

other in-house or third-party systems) shall be included in the list of authorised connections from the outside.

- A description of the approach to client environment segregation in cases where the Institution's IT resources are shared, e.g. resources managed by cloud service providers and/or intra-group service providers.

- A description of the physical security measures and mechanisms, taking into consideration both those implemented in the Institution's own premises, offices and data centres and those implemented in the service providers to which important operational functions have been outsourced.

- The information relating to the security of payment processes shall include the following aspects:
    - the authentication elements to be made available to payment service users (e.g. username and password, elements classed as possession factors based on OTPs, etc.), along with a description of the envisaged implementation for each of them, also taking into account the underlying payment instruments;
    - for each of the identified authentication elements, a description of how their secure delivery to the legitimate payment service user and the integrity of authentication factors, such as hardware tokens and mobile applications, will be ensured, bearing in mind both the initial sign-up and the possible renewals;
    - a description of all the transactions that payment service users can conduct (e.g. accessing payment accounts, issuing transfers, etc.), including the authentication method envisaged (strong customer authentication, planned exemptions, etc.); and
    - a description of the systems and procedures to be applied by the Institution for analysing transactions and identifying those suspicious or unusual, indicating, among other aspects, whether they are systems developed in-house or by third parties, the different factors used for detecting suspicious transactions (e.g. the transaction amount, patterns of behaviour such as the geographical location, usual transactions, etc.) or examples of the most relevant rules for detecting such transactions. This is irrespective of the systems and procedures to be implemented to comply with the obligations established for the prevention of money laundering and terrorist financing.

These security control and risk mitigation measures must indicate how they ensure a high level of technical security and data protection, both in relation to the software and IT systems used by the Institution and to those used by the undertakings to which it outsources all or part of its operations, including, but not limited to, the group's service providers and cloud service providers. These measures shall also include the security measures established in Chapter V "Operational and security risks" of RDL 19/2018.

In drafting the security policy, the Institution must take into account the provisions of the EBA/GL/2019/04 Guidelines of 28 November 2019 on ICT and security risk management.

2.13 INTERNAL CONTROL MECHANISMS TO COMPLY WITH OBLIGATIONS IN RELATION TO MONEY LAUNDERING AND TERRORIST FINANCING

A description must be provided of the internal control mechanisms, procedures and bodies that the Institution intends to establish in order to prevent and deter money laundering or terrorist financing operations.

2.14 IDENTITY AND SUITABILITY ASSESSMENT OF PERSONS WITH QUALIFYING HOLDINGS

The persons who have or will have a qualifying holding in the Institution must be identified, as well as the amount of this holding and whether it is direct or indirect.

A qualifying holding is deemed to be one that represents, directly or indirectly, at least 10% of the Institution's capital or voting rights and one that, without reaching the indicated percentage, allows the exercise of significant influence[7] over the Institution. The indirect holding must be calculated in accordance with the criteria set out in Section 6 of the Joint Guidelines on the prudential assessment of acquisitions and increases of qualifying holdings in the financial sector (JC/GL/2016/01); in particular, the control and the multiplication criteria should be applied, as indicated in the aforementioned section, along each branch of the corporate chain.

Whether the person with a direct or indirect qualifying holding is a natural or a legal person, the corresponding documentation must be completed, pursuant to the form available at the Banco de España's Virtual Office:

- Form for suitability of partners or shareholders with a qualifying holding

The form submitted must be validated and duly signed by the partner or shareholder with a qualifying holding themselves or by a person who can prove they have sufficient representative powers.

When the partner or shareholder with a direct or indirect qualifying holding is a legal person, a Form for suitability of the persons who effectively run the business of the partner or shareholder with a qualifying holding (legal person) must also be submitted for each such director or manager.

Both if the partner or shareholder with a qualifying holding is a natural person or a legal person, it must be confirmed whether there are or will be any concerted arrangements such as agreements or qualified majorities among the Institution's shareholders and, if this is the case, a description of these or a copy of the agreement, if any, must be provided.

[7] Significant influence means being able to appoint or remove a member of the Institution's management body. However, Section 5 of the JC/GL/2016/01 sets out a non-exhaustive list of factors to determine whether a proposal for the acquisition of a holding would allow the proposed acquirer to exercise a significant influence on the management of the target undertaking.

In addition, except in the cases mentioned below, the annual accounts of the partner or shareholder with a qualifying holding (which must be audited if so required) must be provided.

If the partner or shareholder with a direct or indirect qualifying holding is an institution supervised by the Banco de España, only Sections 5 to 7 of the Form for suitability of the partner or shareholder with a qualifying holding need be completed, and it shall not be necessary to provide the institution's financial statements or to provide the Forms for suitability of the persons effectively running its business, provided that they have not changed and are the same as those previously assessed. However, a signed statement must be submitted certifying that there have been no changes with regard to the documentation already on file at the Banco de España or that may have an impact on the suitability assessment.

Conversely, if the partner or shareholder with a direct or indirect qualifying holding is an institution supervised by the National Securities Market Commission (CMNV), the Directorate General of Insurance and Pension Funds or another European supervisory authority other than the Banco de España, only Sections 1 and 3 to 7 of the Form for suitability of the partner of shareholder with a qualifying holding need be completed, and the institution's financial statements must be provided along with the Forms for suitability of the persons effectively running its business. This is without prejudice to further information requests if deemed necessary.

2.15 IDENTITY AND SUITABILITY ASSESSMENT OF DIRECTORS AND PERSONS RESPONSIBLE FOR MANAGEMENT

The Applicant must identify the directors and general managers responsible for the management and the provision of payment services and, where appropriate, for the issuance of electronic money.

For each of these persons, the corresponding documentation must be completed, in accordance with the form available at the Banco de España's Virtual Office:

- Questionnaire for assessing the suitability of senior officers (institutions other than credit institutions and specialised lending institutions)

2.16 IDENTITY OF EXTERNAL STATUTORY AUDITOR

The auditor who will be responsible for auditing the Institution's financial statements must be identified.

2.17 CUSTOMER SERVICE DEPARTMENT

The head of the Institution's customer service department ("**CSD**") must be identified, and the CSD's contact details (postal and e-mail address) must be provided.

A report must be provided describing the measures that the Institution will adopt to separate the CSD from the other commercial and operating services of the organisation, so that it can take its decisions autonomously and conflicts of interest are avoided.

Also to be provided are the customer ombudsman rules, prepared in accordance with the provisions of Ministry of Economy Order ECO/734/2004 of 11 March 2004 on customer care departments and services and the customer ombudsmen of financial institutions, bearing in mind the time limits set out in Article 69 of RDL 19/2018 for payment service complaints..

If the Institution intends to advertise banking products and services included within the objective scope of Rule 3 of Banco de España Circular 4/2020 of 26 June 2020 on the advertising of banking products and services, it must notify the Banco de España and, when so required, submit the commercial communication policy.

2.18 PROFESSIONAL INDEMNITY INSURANCE OR COMPARABLE GUARANTEE

If the Institution is going to provide payment initiation services (Article 1.2(g) of RDL 19/2018) and/or account information services (Article 1.2(h) of RDL 19/2018) exclusively or with other payment services, it must provide evidence of the existence of professional indemnity insurance, bank guarantee or other equivalent guarantee in the opinion of the Banco de España, to be provided by a credit institution or insurer authorised to provide services in Spain and that does not belong the same group as the Institution. If the Institution is only going to provide account information services, Section 3.12 of this Guide shall apply.

The Applicant must provide a draft of the professional civil indemnity insurance policy or equivalent guarantee, the terms of which must comply with the following, taking into account whether the Institution will provide the payment initiation service, the account information service, or both services together:

- It must specify that it covers the provision on a professional basis of payment initiation and/or account information services.

- In particular, it must cover any liabilities that may arise from the payment initiation activity under Articles 45 (execution of unauthorised payment transactions), 61 (non-execution or defective execution of payment transactions) and 63 (right to damages) of RDL 19/2018 and/or from the account information activity arising from non-authorised or fraudulent access to or non-authorised or fraudulent use of payment account information.

- It must cover, at least, the monetary amount calculated in accordance with the EBA GL/2017/08 Guidelines for which the EBA tool may be used (the "**Minimum Monetary Amount**"). An explication must be provided of the assumptions used in the calculation.

- In the event that the amount of the cover includes any excess, deductible or threshold, these should not prejudice repayments that the Institution must make resulting from the requests for refunds of payment service users and/or account servicing payment service providers. Such excess, deductible or threshold shall be covered by a safeguard. For this purpose, Banco de España will take into account the submission by the Applicant of safeguards that cover the amount of the excess, deductible or threshold at all times throughout the life of the insurance, such as:

    - In the event that the policy includes an aggregate excess, the constitution of an unavailable deposit for the maximum aggregate excess amount (the amount of the excess multiplied by the number of times it would be applicable) contained in the policy.

    - In the event that the Institution had demonstrable difficulties in taking out a policy with an aggregate excess, the deposit would cover four times the amount of the excess included in the policy.

    - In both cases, in order to prove that the safeguard exists, the Institution may send a declaration, in the terms set out in Article 69 of Law 39/2015 of 1 October 2015 on the Common Administrative Procedure for General Government, specifically stating that such deposit in the name of the Institution exists, including as an annex the certificate issued by the bank confirming the account number and amount, and that the Institution undertakes to use it only to meet the payments it may have to make as a result of the excess of the professional indemnity insurance.

- If the policy provides for the possibility of paying the premium in instalments, this must not affect the payments to be made by the Institution in relation to the reimbursement requests made by the payment service users and/or by the payment service providers who manage the account throughout the period of cover.

- There must be no (i) coverage for liabilities other than that indicated above, or (ii) sub-limits on liabilities that may arise from the payment initiation and/or account information activity, that may reduce the amount of professional civil indemnity coverage for the covered payment services below the Minimum Monetary Amount. When the policy includes additional liabilities other than those contained in RDL 19/2018, it must include a limit reinstatement clause for these cases, so that they are covered at all times.

- It must not include exceptions that apply to the payment service user or account servicing payment service provider.

- It must establish that, if the policy or equivalent guarantee is not renewed or replaced, it will have to provide cover for at least thirteen months immediately following the termination date.

- It must establish that, for the purpose of applying the insured amount, all claims deriving from the same event giving rise to civil liability shall be deemed to be one single claimable event.

- It must cover the exercise of the Institution's professional activity in the territories in which it is going to offer services.

- It must be subject to Spanish law and jurisdiction, notwithstanding the provisions of Article 107.2 of Law 50/1980 of 8 October 1980 on the insurance contract.

3 REGISTRATION OF NATURAL OR LEGAL PERSONS PROVIDING ACCOUNT INFORMATION SERVICES

This section is applicable to natural or legal persons having their central administration, registered office or, where applicable, place of residence in Spain for which registration is applied in order to provide, from among the payment services, exclusively the account information payment service on a professional basis in Spain.

The registration regime of natural or legal persons providing the account information service is regulated by Article 15 of RDL 19/2018. As regards documentation requirements, Article 3 of RD 736/2019 must be taken into account.

The Banco de España has prepared the following form whose sections identify the information that must accompany the application:

- Form for registration of natural or legal persons providing account information service

Following is a detailed description of the specific sections of the form, specifying some of the matters that give rise to doubts most frequently.

3.1 IDENTIFICATION DETAILS

If the application for registration is for a natural person who will provide account information services, his/her identification details must be provided together with a copy of (i) his/her national identity card or equivalent document, (ii) updated curriculum vitae, and (iii) criminal record certificate not older than three months.

Whether the application is for a legal person or a natural person, the information mentioned in Section 2.1 of this Guide must also be provided.

3.2 PROGRAMME OF OPERATIONS

A report must be submitted explaining the service to be provided, including the processing of data, and how it fits the definition of account information service, i.e. '*online service to provide consolidated information on one or more payment accounts held by the payment*

service user with either another payment service provider or with more than one payment service provider'.

In addition, details should be provided on how customer data and access credentials will be used and how consent will be obtained, as well as the parties/entities involved in these data flows or credentials.

The remaining information referred to in Section 2.2 of this Guide must also be provided.

3.3 BUSINESS PLAN

The information mentioned in Section 2.3 of this Guide must be provided, although, since Article 19 of RDL 19/2018 is not applicable, it shall not be necessary to provide information on required own funds.

3.4 STRUCTURAL ORGANIZATION

The information mentioned in Section 2.4 of this Guide must be provided, although it shall not be necessary to provide a description of the structural organisation in the same terms as a legal person if the person for whom registration is applied is a natural person, nor information on close links whether a natural or legal person.

3.5 CORPORATE GOVERNANCE PROCEDURES AND INTERNAL CONTROL MECHANISMS

The information mentioned in Section 2.7 of this Guide must be provided.

3.6 PROCEDURE FOR MONITORING, HANDLING AND FOLLOWING UP ON SECURITY INCIDENTS AND SECURITY-RELATED CUSTOMER COMPLAINTS

The information mentioned in Section 2.8 of this Guide must be provided.

3.7 PROCESS IN PLACE TO FILE, MONITOR, TRACK AND RESTRICT ACCESS TO SENSITIVE PAYMENT DATA

The information mentioned in Section 2.9 of this Guide must be provided.

3.8 BUSINESS CONTINUITY ARRANGEMENTS

The information mentioned in Section 2.10 of this Guide must be provided.

3.9 SECURITY POLICY DOCUMENT

The information mentioned in Section 2.12 of this Guide must be provided.

3.10 IDENTITY AND SUITABILITY ASSESSMENT OF DIRECTORS AND PERSONS RESPONSIBLE FOR MANAGEMENT

The information mentioned in Section 2.15 of this Guide must be provided.

3.11 CUSTOMER SERVICE DEPARTMENT

The information mentioned in Section 2.17 of this Guide must be provided.

3.12 PROFESSIONAL INDEMNITY INSURANCE OR COMPARABLE GUARANTEE

The information mentioned in Section 2.18 of this Guide must be provided and the insurance policy or guarantee must cover in particular the liabilities that may arise from account information activity resulting from non-authorised or fraudulent access to or non-authorised or fraudulent use of payment account information.

4 REGISTRATION OF NATURAL OR LEGAL PERSONS EXEMPT FROM THE LEGAL REGIME APPLICABLE TO PAYMENT INSTITUTIONS REFERRED TO IN ARTICLE 14 OF ROYAL DECREE-LAW 19/2018

This section is applicable to natural or legal persons having their central administration, registered office or, where applicable, place of residence in Spain for which registration is applied to provide payment services (except for the payment initiation service (Article 1.2 g) of RDL 19/2018) and/or the account information service (Article 1.2 h) of RDL 19/2018) under the exemption regime provided for in Article 14 of RDL 19/2018.

In accordance with the provisions of Article 14 of RDL 19/2018, the Banco de España is responsible for verifying (i) compliance with the provisions of Article 14.1 and 2 of RDL 19/2018, and (ii) the provision of the documentation indicated in Article 4.1 of RD 736/2019, prior to the registration of the Institution as exempt from the legal regime applicable to payment institutions in the Banco de España's Special Registry.

As regards the provision of the documentation indicated in Article 4.1 of RD 736/2019, the Banco de España shall merely carry out a formal check on the documentation submitted, which will in no way validate it or limit the freedom of action of both the Banco de España and the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences. Therefore, the Institution's registration shall be understood to be without prejudice to the fact that, within the framework of the Institution's supervision, compliance with the obligations corresponding to it as a payment service provider shall be reviewed, and the Institution shall have to correct any shortcomings identified.

The Banco de España has prepared the following form whose sections identify the information that must accompany the application:

- Form for registration of natural or legal persons with a low volume of business

Following is a detailed description of the specific sections of the form, specifying some of the matters that give rise to doubts most frequently.

4.1 Identification details

The Institution's identification details must be provided whether it is a natural or legal person.

4.2 Registration conditions

It must be confirmed that the Institution complies with the provisions of Article 14.1 and 2 of RDL 19/2018 and Article 4.1 of RD 736/2019, i.e.:

- That the Institution will not provide the payment initiation or account information services referred to in Article 1.2(g) and (h) of RDL 19/2018.
- That the central administration or place of residence of the Institution will be established in Spain.
- That the Institution will not exercise the freedom of establishment or the freedom to provide services in the rest of the European Union.
- That the average total value projected for the first twelve months of the payment transactions performed by the Institution will not exceed EUR 3 million per month. This requirement will be assessed with respect to the total amount of payment transactions projected in its business plan, unless the Banco de España requires the modification of that plan.
- That none of the natural persons responsible for the management or exercise of the Institution's activity have been convicted of money laundering or terrorist financing or other financial crimes.
- That the Institution has provided the documentation referred to in Sections 4.3 to 4.11 of this Guide as well as the criminal record certificate of the natural persons responsible for managing or providing the Institution's activity.

4.3 Programme of operations

The information referred to in Section 2.2 of this Guide must be provided.

4.4 Business Plan

The information referred to in Section 2.3 of this Guide must be provided, although, as Article 19 of RDL 19/2018 is not applicable, it shall not be necessary to provide information on the own funds required, unless the Institution grants credit in relation to the payment services referred to in Article 1.2(d) or (e) of RDL 19/2018.

4.5 Procedure for monitoring, handling and following up on security incidents and security-related customer complaints

The information mentioned in Section 2.8 of this Guide must be provided.

4.6 Process in place to file, monitor, track and restrict access to sensitive payment data

The information mentioned in Section 2.9 of this Guide must be provided.

4.7 The principles and definitions applicable to the collection of statistical data on performance, transactions and fraud

The information mentioned in Section 2.11 of this Guide must be provided.

4.8 Security policy document

The information mentioned in Section 2.12 of this Guide must be provided.

4.9 Internal control mechanisms to comply with obligations in relation to money laundering and terrorist financing

The information mentioned in Section 2.13 of this Guide must be provided.

4.10 Measures to safeguard users' funds

Natural or legal persons that avail themselves of the regime provided for in Article 14 of RDL 19/2018 are obliged to comply with the guarantee requirements set out in Article 16 of RDL 19/2018, whenever they provide payment services other than money remittance. In any case, Banco de España will require compliance with the aforementioned guarantee requirements at any time when, in its opinion, it is necessary to guarantee the protection of payment services user and confidence in the payment systems.

If case of safeguarding the funds, the information mentioned in Section 2.6 of this Guide must be provided.

4.11 Customer service department

The information mentioned in Section 2.17 of this Guide must be provided.

****