EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers

(EBA/GL/2017/09)

These guidelines are addressed to competent authorities, as defined in point (i) of Article 4(2) of Regulation (EU) No 1093/2010, and to the following financial institutions: payment institutions as defined in point (4) of Article 4 of Directive (EU) 2015/2366; electronic money institutions as defined in point (1) of Article 2 of Directive 2009/110/EC; and account information service providers as defined in point (19) of Article 4 of Directive (EU) 2015/2366.

These guidelines set out the information to be provided to the competent authorities in the application for the authorisation of payment institutions, in the application for registration of account information service providers and in the application for authorisation of electronic money institutions.

The information provided by applicants should be true, complete, accurate and up to date. All applicants should comply with all the provisions in the set of guidelines that applies to them. The level of detail should be proportionate to the applicant's size and internal organisation, and to the nature, scope, complexity and riskiness of the particular service(s) that the applicant intends to provide.

These Guidelines have been developed by the EBA in accordance with article 16 of Regulation (EU) No 1093/2010. The EBA published the English version of these Guidelines on 11 July 2017 (the Spanish version was released on 13 January 2018). The Guidelines apply from 13 January 2018.

The Executive Commission of the Banco de España, in its role of competent authority for the authorization of payment institutions and electronic money institutions and the register of providers of account information services, adopted these Guidelines as their own on 19 March 2019.

EBA/GL/2017/09

08/11/2017

Guidelines

on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers under Article 5(5) of Directive (EU) 2015/2366

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[1]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

Reporting requirements

3. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA that they comply or intend to comply with these guidelines, or otherwise give reasons for non-compliance, by 08/01/2018. In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2017/09'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

2. Subject matter, scope and definitions

Subject matter

5. These guidelines set out the information to be provided to the competent authorities in the application for the authorisation of payment institutions, in the application for registration of account information service providers and in the application for authorisation of electronic money institutions.

Scope of application

6. These guidelines apply in relation to: (a) applications for authorisation as a payment institution in accordance with Article 5 of Directive (EU) 2015/2366; (b) registration as an account information service provider, in accordance with Article 5 and Article 33 of Directive (EU) 2015/2366; and (c) applications for authorisation as an electronic money institution, by virtue of the application *mutatis mutandis* of Article 5 of Directive (EU) 2015/2366 to electronic money institutions, in accordance with Article 3(1) of Directive 2009/110/EC.

Addressees

7. These guidelines are addressed to competent authorities, as defined in point (i) of Article 4(2) of Regulation (EU) No 1093/2010, and to the following financial institutions: payment institutions as defined in point (4) of Article 4 of Directive (EU) 2015/2366; electronic money institutions as defined in point (1) of Article 2 of Directive 2009/110/EC; and account information service providers as defined in point (19) of Article 4 of Directive (EU) 2015/2366.

Definitions

8. The terms used and defined in Directive (EU) 2015/2366 and Directive 2009/110/EC have the same meaning in the guidelines.

3. Implementation

Date of application

9. These guidelines apply from 13 January 2018.

4. Four sets of Guidelines, applicable to payment institutions (PIS), account information services providers (AISPs), electronic money institutions (EMIs), and competent authorities (CAs) respectively

4.1. Guidelines on the information required from applicants for authorisation as payment institutions for the provision of services 1-8 of Annex I to Directive (EU) 2015/2366

Guideline 1: General principles

1.1 This set of guidelines applies to applicants for authorisation as payment institutions (PIs). This includes applicants that intend to provide any service(s) referred to in points 1-7 of Annex I to PSD2 or service 8 in combination with other payment services. Applicants that intend to provide only the service referred to in point 8 of Annex I to Directive (EU) 2015/2366 (PSD2) are subject to the specific set of guidelines for account information service providers (AISPs) set out in section 4.2.

1.2 The information provided by applicants should be true, complete, accurate and up to date. All applicants should comply with all the provisions in the set of guidelines that applies to them. The level of detail should be proportionate to the applicant's size and internal organisation, and to the nature, scope, complexity and riskiness of the particular service(s) that the applicant intends to provide. In any event, in accordance with Directive (EU) 2015/2366, the directors and the persons responsible for the management of the payment institution are of good repute and possess appropriate knowledge and experience to perform payment services, regardless of the institution's size, internal organisation and the nature, scope and complexity of its activities and the duties and responsibilities of the specific position.

1.3 When submitting the information required, the applicant should avoid making references to specific sections of internal procedures/documents. Instead, the applicant should extract the relevant sections and provide these to the competent authority (CA).

1.4 Should the CAs require clarifications on the information that has been submitted, the applicant should provide such clarification without delay.

1.5 All data requested under these guidelines for authorisations as payment institutions are needed for the assessment of the application and will be treated by the CA in accordance with the professional secrecy obligations set out in PSD2, without prejudice to applicable

Union law and national requirements and procedures on the exercise of the right to access, rectify, cancel or oppose.

Guideline 2: Identification details

2.1 The identification details to be provided by the applicant should contain the following information:

a) the applicant's corporate name and, if different, trade name;

b) an indication of whether the applicant is already incorporated or in process of incorporation;

c) the applicant's national identification number, if applicable;

d) the applicant's legal status and (draft) articles of association and/or constitutional documents evidencing the applicant's legal status;

e) the address of the applicant's head office and registered office;

f) the applicant's electronic address and website, if available;

g) the name(s) of the person(s) in charge of dealing with the application file and authorisation procedure, and their contact details;

h) an indication of whether or not the applicant has ever been, or is currently being, regulated by a competent authority in the financial services sector;

i) any trade association(s) in relation to the provision of payment services that the applicant plans to join, where applicable;

j) the register certificate of incorporation or, if applicable, negative certificate of a mercantile register that certifies that the name applied by the company is available;

k) evidence of the payment of any fees or of the deposit of funds to file an application for authorisation as a payment institution, where applicable under national law.

Guideline 3: Programme of operations

3.1. The programme of operations to be provided by the applicant should contain the following information:

a) a step-by-step description of the type of payment services envisaged, including an explanation of how the activities and the operations that will be provided are identified

by the applicant as fitting into any of the legal categories of payment services listed in Annex I to PSD2.

b) a declaration of whether the applicant will at any point enter or not into possession of funds;

c) a description of the execution of the different payment services, detailing all parties involved, and including for each payment service provided:

   i. a diagram of flow of funds, unless the applicant intends to provide payment initiation services (PIS) only;

   ii. settlement arrangements, unless the applicant intends to provide PIS only;

   iii. draft contracts between all the parties involved in the provision of payment services including those with payment card schemes, if applicable;

   iv. processing times.

d) a copy of the draft framework contract, as defined in Article 4(21) of PSD2;

e) the estimated number of different premises from which the applicant intends to provide the payment services, and/or carry out activities related to the provision of the payment services, if applicable;

f) a description of any ancillary services to the payment services, if applicable;

g) a declaration of whether or not the applicant intends to grant credit and, if so, within which limits;

h) a declaration of whether or not the applicant plans to provide payment services in other Member States or third countries after the granting of the licence;

i) an indication of whether or not the applicant intends, for the next three years, to provide or already provides other business activities as referred to in Article 18 of Directive (EU) 2015/2366, including a description of the type and expected volume of the activities;

j) the information specified in the EBA Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366 where the applicant intends to provide services 7 and 8 (PIS and account information services (AIS).

Guideline 4: Business plan

4.1. The business plan to be provided by the applicant should contain:

a) a marketing plan consisting of:

i. an analysis of the company's competitive position in the payment market segment concerned;

ii. a description of the payment service users, marketing materials and distribution channels;

b) where available for existing companies, certified annual accounts for the previous three years, or a summary of the financial situation for those companies that have not yet produced annual accounts;

c) a forecast budget calculation for the first three financial years that demonstrates that the applicant is able to employ appropriate and proportionate systems, resources and procedures that allow the applicant to operate soundly; it should include:

i. an income statement and balance-sheet forecast, including target scenarios and stress scenarios as well as their base assumptions, such as volume and value of transactions, number of clients, pricing, average amount per transaction, expected increase in profitability threshold;

ii. explanations of the main lines of income and expenses, the financial debts and the capital assets;

iii. a diagram and detailed breakdown of the estimated cash flows for the next three years;

d) information on own funds, including the amount and detailed breakdown of the composition of initial capital as set out in Article 7 of PSD2;

e) information on, and calculation of, minimum own funds requirements in accordance with the method(s) referred to in Article 9 of Directive (EU) 2015/2366 (PSD2) as determined by the competent authority, unless the applicant intends to provide PIS only, including:

i. an annual projection of the breakdown of the own funds for three years according to the method used;
ii. an annual projection of the own funds for three years according to the other methods.

Guideline 5: Structural organisation

5.1. The applicant should provide a description of the structural organisation of its undertaking consisting of:

a) a detailed organisational chart, showing each division, department or similar structural separation, including the name of the person(s) responsible, in particular those in charge of internal control functions; the chart should be accompanied by descriptions of the functions and responsibilities of each division, department or similar structural separation;

b) an overall forecast of the staff numbers for the next three years;

c) a description of relevant operational outsourcing arrangements consisting of:

i. the identity and geographical location of the outsourcing provider;

ii. the identity of the persons within the payment institution that are responsible for each of the outsourced activities;

iii. a clear description of the outsourced activities and their main characteristics;

d) a copy of draft outsourcing agreements;

e) a description of the use of branches and agents, where applicable, including:

i. a mapping of the off-site and on-site checks that the applicant intends to perform, at least annually, on branches and agents and their frequency;

ii. the IT systems, the processes and the infrastructure that are used by the applicant's agents to perform activities on behalf of the applicant;

iii. in the case of agents, the selection policy, monitoring procedures and agents' training and, where available, the draft terms of engagement;

iv. an indication of the national and/or international payment system that the applicant will access, if applicable;

f) a list of all natural or legal persons that have close links with the applicant, indicating their identities and the nature of those links.

Guideline 6: Evidence of initial capital

6.1. For the evidence of initial capital to be provided by the applicant (of EUR 125 000 for services 1-5 of Annex I to PSD2; EUR 20 000 for service 6; and EUR 50 000 for service 7), the applicant should submit the following documents:

a) for existing undertakings, an audited account statement or public register certifying the amount of capital of the applicant;

b) for undertakings in the process of being incorporated, a bank statement issued by a bank certifying that the funds are deposited in the applicant's bank account.

Guideline 7: Measures to safeguard the funds of payment service users (applicable to payment services 1-6 only)

7.1. Where the applicant safeguards the payment service users' funds through depositing funds in a separate account in a credit institution or through an investment in secure, liquid, low-risk assets, the description of the safeguarding measures should contain:

a) a description of the investment policy to ensure the assets chosen are liquid, secure and low risk, if applicable;

b) the number of persons that have access to the safeguarding account and their functions;

c) a description of the administration and reconciliation process to ensure that payment service users' funds are insulated in the interest of payment service users against the claims of other creditors of the payment institution, in particular in the event of insolvency;

d) a copy of the draft contract with the credit institution;

e) an explicit declaration by the payment institution of compliance with Article 10 of PSD2.

7.2. Where the applicant safeguards the funds of the payment service user through an insurance policy or comparable guarantee from an insurance company or a credit institution, the description of the safeguarding measures should contain the following:

a) a confirmation that the insurance policy or comparable guarantee from an insurance company or a credit institution is from an entity that is not part of the same group of firms as the applicant;

b) details of the reconciliation process in place to ensure that the insurance policy or comparable guarantee is sufficient to meet the applicant's safeguarding obligations at all times;

c) duration and renewal of the coverage;

d) a copy of the (draft) insurance agreement or the (draft) comparable guarantee.

Guideline 8: Governance arrangements and internal control mechanisms

8.1. The applicant should provide a description of the governance arrangement and the internal control mechanisms consisting of:

a) a mapping of the risks identified by the applicant, including the type of risks and the procedures the applicant will put in place to assess and prevent such risks;

b) the different procedures to carry out periodical and permanent controls including the frequency and the human resources allocated;

c) the accounting procedures by which the applicant will record and report its financial information;

d) the identity of the person(s) responsible for the internal control functions, including for periodic, permanent and compliance control, as well as an up-to-date curriculum vitae;

e) the identity of any auditor that is not a statutory auditor pursuant to Directive 2006/43/EC;

f) the composition of the management body and, if applicable, of any other oversight body or committee;

g) a description of the way outsourced functions are monitored and controlled so as to avoid an impairment in the quality of the payment institution's internal controls;

h) a description of the way any agents and branches are monitored and controlled within the framework of the applicant's internal controls;

i) where the applicant is the subsidiary of a regulated entity in another EU Member State, a description of the group governance.

Guideline 9: Procedure for monitoring, handling and following up on security incidents and security-related customer complaints

9.1. The applicant should provide a description of the procedure in place to monitor, handle and follow up on security incidents and security-related customer complaints to be provided by the applicant, which should contain:

a) organisational measures and tools for the prevention of fraud;

b) details of the individual(s) and bodies responsible for assisting customers in cases of fraud, technical issues and/or claim management;

c) reporting lines in cases of fraud;

d) the contact point for customers, including a name and email address;

e) the procedures for the reporting of incidents, including the communication of these reports to internal or external bodies, including notification of major incidents to national competent authorities under Article 96 of PSD2, and in line with the EBA guidelines on incident reporting under the referred Article.

f) the monitoring tools used and the follow-up measures and procedures in place to mitigate security risks.

Guideline 10: Process for filing, monitoring, tracking and restricting access to sensitive payment data

10.1. The applicant should provide a description of the process in place to file, monitor, track and restrict access to sensitive payment data consisting of:

a) a description of the flows of data classified as sensitive payment data in the context of the payment institution's business model;

b) the procedures in place to authorise access to sensitive payment data;

c) a description of the monitoring tool;

d) the access right policy, detailing access to all relevant infrastructure components and systems, including databases and back-up infrastructures;

e) unless the applicant intends to provide PIS only, a description of how the collected data are filed;

f) unless the applicant intends to provide PIS only, the expected internal and/or external use of the collected data, including by counterparties;

g) the IT system and technical security measures that have been implemented including encryption and/or tokenisation;

h) identification of the individuals, bodies and/or committees with access to the sensitive payment data;

i) an explanation of how breaches will be detected and addressed;

j) an annual internal control programme in relation to the safety of the IT systems.

Guideline 11: Business continuity arrangements

11.1. The applicant should provide a description of the business continuity arrangements consisting of the following information:

a) a business impact analysis, including the business processes and recovery objectives, such as recovery time objectives, recovery point objectives and protected assets;

b) the identification of the back-up site, access to IT infrastructure, and the key software and data to recover from a disaster or disruption;

c) an explanation of how the applicant will deal with significant continuity events and disruptions, such as the failure of key systems; the loss of key data; the inaccessibility of the premises; and the loss of key persons;

d) the frequency with which the applicant intends to test the business continuity and disaster recovery plans, including how the results of the testing will be recorded;

e) a description of the mitigation measures to be adopted by the applicant, in cases of the termination of its payment services, ensuring the execution of pending payment transactions and the termination of existing contracts.

Guideline 12: The principles and definitions applicable to the collection of statistical data on performance, transactions and fraud

12.1. The applicant should provide a description of the principles and definitions applicable to the collection of the statistical data on performance, transactions and fraud consisting of the following information:

a) the type of data that is collected, in relation to customers, type of payment service, channel, instrument, jurisdictions and currencies;

b) the scope of the collection, in terms of the activities and entities concerned, including branches and agents;

c) the means of collection;

d) the purpose of collection;

e) the frequency of collection;

f) supporting documents, such as a manual, that describe how the system works.

Guideline 13: Security policy document

13.1. The applicant should provide a security policy document containing the following information:

a) a detailed risk assessment of the payment service(s) the applicant intends to provide, which should include risks of fraud and the security control and mitigation measures taken to adequately protect payment service users against the risks identified;

b) a description of the IT systems, which should include:

i. the architecture of the systems and their network elements;

ii. the business IT systems supporting the business activities provided, such as the applicant's website, wallets, the payment engine, the risk and fraud management engine, and customer accounting;

iii. the support IT systems used for the organisation and administration of the applicant, such as accounting, legal reporting systems, staff management, customer relationship management, e-mail servers and internal file servers;

iv. information on whether those systems are already used by the applicant or its group, and the estimated date of implementation, if applicable;

c) the type of authorised connections from outside, such as with partners, service providers, entities of the group and employees working remotely, including the rationale for such connections;

d) for each of the connections listed under point c), the logical security measures and mechanisms in place, specifying the control the applicant will have over such access as well as the nature and frequency of each control, such as technical versus organisational; preventative versus detective; and real-time monitoring versus regular reviews, such as the use of an active directory separate from the group, the opening/closing of communication lines, security equipment configuration, generation of keys or client authentication certificates, system monitoring, authentication, confidentiality of communication, intrusion detection, antivirus systems and logs;

e) the logical security measures and mechanisms that govern the internal access to IT systems, which should include:

i. the technical and organisational nature and frequency of each measure, such as whether it is preventative or detective and whether or not it is carried out in real time;

ii. how the issue of client environment segregation is dealt with in cases where the applicant's IT resources are shared;

f) the physical security measures and mechanisms of the premises and the data centre of the applicant, such as access controls and environmental security;

g) the security of the payment processes, which should include:

i. the customer authentication procedure used for both consultative and transactional access, and for all underlying payment instruments;

ii. an explanation of how safe delivery to the legitimate payment service user and the integrity of authentication factors, such as hardware tokens and mobile applications, are ensured, at the time of both initial enrolment and renewal;

iii. a description of the systems and procedures that the applicant has in place for transaction analysis and the identification of suspicious or unusual transactions;

h) a detailed risk assessment in relation to its payment services, including fraud, with a link to the control and mitigation measures explained in the application file, demonstrating that the risks are addressed;

i) a list of the main written procedures in relation to the applicant's IT systems or, for procedures that have not yet been formalised, an estimated date for their finalisation.

Guideline 14: Internal control mechanisms to comply with obligations in relation to money laundering and terrorist financing (AML/CFT obligations)

14.1. The description of the internal control mechanisms that the applicant has established in order to comply, where applicable, with those obligations should contain the following information:

a) the applicant's assessment of the money laundering and terrorist financing risks associated with its business, including the risks associated with the applicant's customer base, the products and services provided, the distribution channels used and the geographical areas of operation;

b) the measures the applicant has or will put in place to mitigate the risks and comply with applicable anti-money laundering and counter terrorist financing obligations, including the applicant's risk assessment process, the policies and procedures to comply with customer due diligence requirements, and the policies and procedures to detect and report suspicious transactions or activities;

c) the systems and controls the applicant has or will put in place to ensure that its branches and agents comply with applicable anti-money laundering and counter terrorist financing requirements, including in cases where the agent or branch is located in another Member State;

d) arrangements the applicant has or will put in place to ensure that staff and agents are appropriately trained in anti-money laundering and counter terrorist financing matters;

e) the identity of the person in charge of ensuring the applicant's compliance with anti-money laundering and counter-terrorism obligations, and evidence that their anti-money laundering and counter-terrorism expertise is sufficient to enable them to fulfil this role effectively;

f) the systems and controls the applicant has or will put in place to ensure that its anti-money laundering and counter terrorist financing policies and procedures remain up to date, effective and relevant;

g) the systems and controls the applicant has or will put in place to ensure that the agents do not expose the applicant to increased money laundering and terrorist financing risk;

h) the anti-money laundering and counter terrorism manual for the staff of the applicant.

Guideline 15: Identity and suitability assessment of persons with qualifying holdings in the applicant

15.1 For the purposes of the identity and evidence of the suitability of persons with qualifying holdings in the applicant payment institution, without prejudice to the assessment in accordance with the criteria, as relevant, introduced with Directive 2007/44/EC and specified in the joint guidelines for the prudential assessment of acquisitions of qualifying holdings (JC/GL/2016/01), the applicant should submit the following information:

a) a description of the group to which the applicant belongs and an indication of the parent undertaking, where applicable;

b) a chart setting out the shareholder structure of the applicant, including:

i) the name and the percentage holding (capital/voting right) of each person that has or will have a direct holding in the share capital of the applicant, identifying those that are considered as qualifying holders and the reason for such qualifications;

ii) the name and the percentage holding (capital/voting rights) of each person that has or will have an indirect holding in the share capital of the applicant,

identifying those that are considered as indirect qualifying holders and the reason for such qualification;

c) a list of the names of all persons and other entities that have or, in the case of authorisation, will have qualifying holdings in the applicant's capital, indicating for each such person or entity:

   i. the number and type of shares or other holdings subscribed or to be subscribed;

   ii. the nominal value of such shares or other holdings.

15.2 Where a person who has or, in the case of authorisation, will have a qualifying holding in the applicant's capital is a natural person, the application should set out all of the following information relating to the identity and suitability of that person:

a) the person's name and name at birth, date and place of birth, citizenship (current and previous), identification number (where available) or passport number, address and a copy of an official identity document;

b) a detailed curriculum vitae stating the education and training, previous professional experience and any professional activities or other functions currently performed;

c) a statement, accompanied by supporting documents, containing the following information concerning the person:

   i. subject to national legislative requirements concerning the disclosure of spent convictions, any criminal conviction or proceedings where the person has been found against and which were not set aside;

   ii. any civil or administrative decisions in matters of relevance to the assessment or authorisation process where the person has been found against and any administrative sanctions or measures imposed as a consequence of a breach of laws or regulations (including disqualification as a company director), in each case which were not set aside and against which no appeal is pending or may be filed;

   iii. any bankruptcy, insolvency or similar procedures;

   iv. any pending criminal investigations;

   v. any civil or administrative investigations, enforcement proceedings, sanctions or other enforcement decisions against the person concerning matters that may be considered relevant to the authorisation to commence the activity of a payment institution or to the sound and prudent management of a payment institution;

vi. where such documents can be obtained, an official certificate or any other equivalent document evidencing whether or not any of the events set out in sub-paragraphs (i)-(v) has occurred in respect of the relevant person;

vii. any refusal of registration, authorisation, membership or licence to carry out trade, business or a profession;

viii. any withdrawal, revocation or termination of a registration, authorisation, membership or licence to carry out trade, business or a profession;

ix. any expulsion by an authority or public sector entity in the financial services sector or by a professional body or association;

x. any position of responsibility with an entity subject to any criminal conviction or proceedings, administrative investigations, sanctions or other enforcement decisions for conduct failings, including in respect of fraud, dishonesty, corruption, money laundering, terrorist financing or other financial crime, or of failure to put in place adequate policies and procedures to prevent such events, held at the time when the alleged conduct occurred, together with details of such occurrences and of the person's involvement, if any, in them;

xi. any dismissal from employment or a position of trust, any removal from a fiduciary relationship (other than as a result of the relevant relationship coming to an end by passage of time) and any similar situation;

d) a list of undertakings that the person directs or controls and of which the applicant is aware of after due and careful enquiry; the percentage of control either direct or indirect in these companies; their status (whether or not they are active, dissolved, etc.); and a description of insolvency or similar procedures;

e) where an assessment of reputation of the person has already been conducted by a competent authority in the financial services sector, the identity of that authority and the outcome of the assessment;

f) the current financial position of the person, including details concerning sources of revenues, assets and liabilities, security interests and guarantees, whether granted or received;

g) a description of any links to politically exposed persons, as defined in Article 3(9) of Directive (EU) 2015/849[2].

[2] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L 141, 5.6.2015, p. 73).

15.3 Where a person or entity who has or, in the case of authorisation, will have a qualifying holding in the applicant's capital (including entities that are not a legal person and which hold or should hold the participation in their own name), the application should contain the following information relating to the identity and suitability of that legal person or entity:

a) name;

b) where the legal person or entity is registered in a central register, commercial register, companies register or similar register that has the same purposes of those aforementioned, a copy of the good standing, if possible, or otherwise a registration certificate;

c) the addresses of its registered office and, where different, of its head office, and principal place of business;

d) contact details;

e) corporate documents or, where the person or entity is registered in another Member State, a summary explaining the main legal features of the legal form or the entity;

f) whether or not the legal person or entity has ever been or is regulated by a competent authority in the financial services sector or other government body;

g) where such documents can be obtained, an official certificate or any other equivalent document evidencing the information set out in paragraphs (a) to (e) issued by the relevant competent authority;

h) the information referred to in Guideline 15(2)(c),15(2)(d) 15(2)(e), 15(2)(f),and 15(2)(g) in relation to the legal person or entity;

i) a list containing details of each person who effectively directs the business of the legal person or entity, including their name, date and place of birth, address, their national identification number, where available, and a detailed curriculum vitae (stating relevant education and training, previous professional experience, any professional activities or other relevant functions currently performed), together with the information referred to in Guideline 15(2)(c) and 15(2)(d) in respect of each such person;

j) the shareholding structure of the legal person, including at least their name, date and place of birth, address and, where available, personal identification number or registration number, and the respective share of capital and voting rights of direct or indirect shareholders or members and beneficial owners, as defined in Article 3(6) of Directive (EU) 2015/849;

k) a description of the regulated financial group of which applicant is a part, or may become a part, indicating the parent undertaking and the credit, insurance and security entities within the group; the name of their competent authorities (on an individual or consolidated basis); and

l) annual financial statements, at the individual and, where applicable, the consolidated and sub-consolidated group levels, for the last three financial years, where the legal person or entity has been in operation for that period (or, if less than three years, the period for which the legal person or entity has been in operation and for which financial statements have been prepared), approved by the statutory auditor or audit firm within the meaning of Directive 2006/43/EC[3], where applicable, including each of the following items:

   i. the balance sheet;

   ii. the profit-and-loss accounts or income statement;

   iii. the annual reports and financial annexes and any other documents registered with the relevant registry or competent authority of the legal person;

m) where the legal person has not been operating for a sufficient period to be required to prepare financial statements for the three financial years immediately prior to the date of the application, the application shall set out the existing financial statements (if any);

n) where the legal person or entity has its head office in a third country, general information on the regulatory regime of that third country as applicable to the legal person or entity, including information on the extent to which the third country's anti-money laundering and counter-terrorist financing regime is consistent with the Financial Action Task Force Recommendations;

o) for entities that do not have legal personality such as a collective investment undertaking, a sovereign wealth fund or a trust, the application shall set out the following information:

   i. the identity of the persons who manage assets and of the persons who are beneficiaries or subscribers;

   ii. a copy of the document establishing and governing the entity including the investment policy and any restrictions on investment applicable to the entity.

[3] Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87-107).

15.4. The application shall set out all of the following information for each natural or legal person or entity who has or, in the case of authorisation, will have a qualifying holding in the capital of the applicant:

a) details of that person's or entity's financial or business reasons for owning that holding and the person's or the entity's strategy regarding the holding, including the period for which the person or the entity intends to hold the holding and any intention to increase, reduce or maintain the level of the holding in the foreseeable future;

b) details of the person's or the entity's intentions in respect of the applicant and of the influence the person or the entity intends to exercise over the applicant, including in respect of the dividend policy, the strategic development and the allocation of resources of the applicant, whether or not it intends to act as an active minority shareholder, and the rationale for such intention;

c) information on the person's or the entity's willingness to support the applicant with additional own funds if needed for the development of its activities or in the case of financial difficulties;

d) the content of any intended shareholder's or member's agreements with other shareholders or members in relation to the applicant;

e) an analysis as to whether or not the qualifying holding will impact in any way, including as a result of the person's close links to the applicant, on the ability of the applicant to provide timely and accurate information to the competent authorities;

f) the identity of each member of the management body or of senior management who will direct the business of the applicant and will have been appointed by, or following a nomination from, such shareholders or members, together with, to the extent not already provided, the information set out in Guideline 16.

15.5. The application should set out a detailed explanation of the specific sources of funding for the participation of each person or entity having a qualifying holding in the applicant's capital, which should include:

a) details on the use of private financial resources, including their availability and (so as to ensure that the competent authority is satisfied that the activity that generated the funds is legitimate) source;

b) details on access to financial markets, including details of financial instruments to be issued;

c) information on the use of borrowed funds, including the name of the lenders and details of the facilities granted, such as maturities, terms, security interests and guarantees, as well as information on the source of revenue to be used to repay such borrowings; where the lender is not a credit institution or a financial institution authorised to grant credit, the applicant should provide to the competent authorities information on the origin of the borrowed funds;

d) information on any financial arrangement with other persons who are shareholders or members of the applicant.

Guideline 16: Identity and suitability assessment of directors and persons responsible for the management of the payment institution

16.1. For the purposes of the identity and suitability assessment of directors and persons responsible for the management of the payment institution, the applicant should provide the following information:

a) personal details, including:

i. their full name, gender, place and date of birth, address and nationality, and personal identification number or copy of ID card or equivalent;

ii. details of the position for which the assessment is sought, whether or not the management body position is executive or non-executive. This should also include the following details:

- the letter of appointment, contract, offer of employment or relevant drafts, as applicable;
- the planned start date and duration of the mandate;
- a description of the individual's key duties and responsibilities;

b) where applicable, information on the suitability assessment carried out by the applicant, which should include details of the result of any assessment of the suitability of the individual performed by the institution, such as relevant board minutes or suitability assessment reports or other documents;

c) evidence of knowledge, skills and experience, which should include a curriculum vitae containing details of education and professional experience, including academic qualifications, other relevant training, the name and nature of all organisations for which the individual works or has worked, and the nature and duration of the functions performed, in particular highlighting any activities within the scope of the position sought;

d) evidence of reputation, honesty and integrity, which should include:

i. criminal records and relevant information on criminal investigations and proceedings, relevant civil and administrative cases, and disciplinary actions, including disqualification as a company director, bankruptcy, insolvency and similar procedures, notably through an official certificate or any objectively reliable source of information concerning the absence of criminal conviction, investigations and proceedings, such as third-party investigations and testimonies made by a lawyer or a notary established in the European Union;

ii. a statement as to whether criminal proceedings are pending or the person or any organisation managed by him or her has been involved as a debtor in insolvency proceedings or comparable proceedings;

iii. information concerning the following:

- investigations, enforcement proceedings or sanctions by a supervisory authority that the individual has been directly or indirectly involved in;

- refusal of registration, authorisation, membership or licence to carry out a trade, business or profession; the withdrawal, revocation or termination of registration, authorisation, membership or licence; or expulsion by a regulatory or government body or by a professional body or association;

- dismissal from employment or a position of trust, fiduciary relationship or similar situation, or having been asked to resign from employment in such a position, excluding redundancies;

- whether or not an assessment of reputation of the individual as an acquirer or a person who directs the business of an institution has already been conducted by another competent authority, including the identity of that authority, the date of the assessment and evidence of the outcome of this assessment, and the consent of the individual, where required, to seek and process such information and use the provided information for the suitability assessment;

- whether or not any previous assessment of the individual, on authority from another, non-financial sector, has already been conducted, including the identity of that authority and evidence of the outcome of such an assessment.

Guideline 17: Identity of statutory auditors and audit firms

The identity of statutory auditors and audit firms as defined in Directive 2006/43/EC to be provided by the applicant, where relevant, should contain the names, addresses and contact details of auditors.

Guideline 18: Professional indemnity insurance or a comparable guarantee for payment initiation services and account information services

As evidence of a professional indemnity insurance or comparable guarantee that is compliant with EBA Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional insurance or other comparable guarantee (EBA/GL/2017/08) and Article 5(2) and 5(3) of PSD2, the applicant for the provision of PIS or AIS should provide the following information:

a) an insurance contract or other equivalent document confirming the existence of professional indemnity insurance or a comparable guarantee, with a cover amount that is compliant with the referred EBA Guidelines, showing the coverage of the relevant liabilities;

b) documentation of how the applicant has calculated the minimum amount in a way that is compliant with the referred EBA Guidelines, including all applicable components of the formula specified therein.

4.2. Guidelines on the information required from applicants for registration for the provision of only service 8 of Annex I to Directive (EU) 2015/2366 (account information services)

Guideline 1: General principles

1.1 This set of guidelines applies to applicants for registration as account information service providers (AISPs). This refers to applicants that intend to provide only account information services (AIS). Should the applicant intend to provide additional services to those of AIS they should apply for authorisation and refer to the guidelines set out in section 4.1 for payment institutions (PIs).

1.2 The information provided by applicants should be true, complete, accurate and up to date. All applicants should comply with all the provisions in the set of guidelines that applies to them. The level of detail required to be compliant should be proportionate to the applicant's size and internal organisation, and to the nature, scope, complexity and riskiness of the particular service(s) that the applicant intends to provide. In any event, in accordance with Directive EU 2015/2366, the directors and the persons responsible for the management of the payment institution are of good repute and possess appropriate knowledge and experience to perform payment services, regardless of the institution's size, internal organisation and the nature, scope and complexity of its activities and the duties and responsibilities of the specific position.

1.3 When submitting the information required, the applicant should avoid making references to specific sections of internal procedures/documents. Instead, the applicant should extract the relevant sections and provide these to the competent authority (CA).

1.4 Should the CAs require clarifications on the information that has been submitted, the applicant should provide such clarification without delay.

1.5 All data requested under these guidelines for registration as account information service providers (AISPs) are needed for the assessment of the application and will be treated by the competent authority in accordance with the professional secrecy obligations set out in PSD2, without prejudice to applicable Union law and national requirements and procedures on the exercise of the right to access, rectify, cancel or oppose.

Guideline 2: Identification details

2.1 If the applicant is a natural person, the identification details to be provided by the applicant should contain the following information:

a) name, address, nationality and date and place of birth;

b) a copy of the identity card or equivalent piece of identification;

c) an updated curriculum vitae;

d) a criminal record check not older than 3 months;

e) the name(s) of the person(s) in charge of dealing with the application file and authorisation procedure, and their contact details.

2.2 If the applicant is a legal person, the identification details to be provided by the applicant should contain the following information:

a) the applicant's corporate name and, if different, trade name;

b) an indication of whether the applicant is already incorporated or in process of incorporation;

c) the applicant's national identification number, if applicable;

d) the applicant's legal status and (draft) articles of association and/or constitutional documents evidencing the applicant's legal status;

e) the address of the applicant's head office and registered office;

f) the applicant's electronic address and website, if available;

g) the name of the person(s) in charge of dealing with the application file and authorisation procedure, and their contact details;

h) an indication of whether or not the applicant has ever been, or is currently being, regulated by a competent authority in the financial services sector;

i) the register certificate of incorporation or, if applicable, negative certificate of a mercantile register that certifies that the name applied by the company is available;

j) evidence of the payment of any fees or of the deposit of funds to file an application for registration as an account information service provider, where applicable under national law.

Guideline 3: Programme of operations

3.1. The programme of operations to be provided by the applicant should contain the following information:

a) a description of the account information service that is intended to be provided, including an explanation of how the applicant determined that the activity fits the definition of account information services as defined in Article 4(16) of Directive (EU) 2015/2366 (PSD2);

b) a declaration of the applicant that they will not enter at any time into possession of funds;

c) a description of the provision of the account information service including:

i. draft contracts between all the parties involved, if applicable;

ii. terms and conditions of the provision of the account information services;

iii. processing times;

d) the estimated number of different premises from which the applicant intends to provide the services, if applicable;

e) a description of any ancillary services to the account information service, if applicable;

f) a declaration of whether or not the applicant intends to provide account information services in another EU Member State or another country once registered;

g) an indication of whether the applicant intends, for the next three years, to provide, or already provides, business activities other than account information services as referred to in Article 18 of Directive 2015/2366, including a description of the type and expected volume of the activities;

h) the information specified in EBA Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366 (EBA/GL/2017/08) where the applicant intends to provide only service 8 (AIS).

Guideline 4: Business plan

4.1. The business plan to be provided by the applicant should contain:

a) a marketing plan consisting of:

i. an analysis of the company's competitive position;

ii. a description of account information service users in the account information market segment concerned, marketing materials and distribution channels;

b) certified annual accounts for the previous three years, if available, or a summary of the financial situation for those applicants that have not yet produced annual accounts;

c) a forecast budget calculation for the first three financial years that demonstrates that the applicant is able to employ appropriate and proportionate systems, resources and procedures that allow the applicant to operate soundly; it should include:

i. an income statement and balance-sheet forecast, including target scenarios and stress scenarios as well as their base assumptions, such as number of clients, pricing and expected increase in profitability threshold;

ii. explanations of the main lines of income and expenses, the financial debts and the capital assets;

iii. a diagram and detailed breakdown of the estimated cash flows for the next three years.

Guideline 5: Structural organisation

5.1. If the applicant is a natural person, the description of the structural organisation of the applicant's undertaking should contain the following information:

a) an overall forecast of the staff numbers for the next three years;

b) a description of the relevant operational outsourcing arrangements consisting of:

i. the identity and geographical location of the outsourcing provider;

ii. the identities of the persons within the AISP that are responsible for each of the outsourced activities;

iii. a detailed description of the outsourced activities and its main characteristics;

c) a copy of draft outsourcing agreements;

d) if applicable, a description of the use of branches and agents, including:

i. a mapping of the off-site and on-site checks that the applicant intends to perform of branches and agents;

ii. the IT systems, processes and infrastructure that are used by the applicant's agents to perform activities on behalf of the applicant;

iii. in the case of agents, the selection policy, monitoring procedures and agents' training and, where available, the draft terms of engagement;

e) a list of all natural or legal persons that have close links with the applicant AISP, indicating their identity and the nature of those links.

5.2. If the applicant is a legal person, the description of the structural organisation of its undertaking should contain the following information:

a) a detailed organisational chart, showing each division, department or similar structural separation, including the name of the person(s) responsible, in particular those in charge of internal control functions; the chart should be accompanied by a description of the functions and responsibilities of each division, department or similar structural separation;

b) an overall forecast of the staff numbers for the next three years;

c) a description of the relevant outsourcing arrangements consisting of:

i. the identity and geographical location of the outsourcing provider;

ii. the identities of the persons within the AISP that are responsible for each of the outsourced activities;

iii. a detailed description of the outsourced activities and its main characteristics;

d) a copy of draft outsourcing agreements;

e) if applicable, a description of the use of branches and agents, including:

i. a mapping of the off-site and on-site checks that the applicant intends to perform of branches and agents;

ii. The IT systems, processes and infrastructures that are used by the applicant's agents to perform activities on behalf of the applicant;

iii. in the case of agents, the selection policy, monitoring procedures and agents' training and, where available, the draft terms of engagement;

f) a list of all natural or legal persons that have close links with the applicant, indicating their identities and the nature of those links.

Guideline 6: Governance arrangements and internal control mechanisms

6.1. The applicant should provide a description of the governance arrangement and internal control mechanisms consisting of:

a) a mapping of the risks identified by the applicant, including the type of risks and the procedures the applicant will put in place to assess and prevent such risks;

b) the different procedures intended to carry out periodical and permanent controls, including the frequency, and the human resources allocated;

c) the accounting procedures by which the applicant will record and report its financial information;

d) the identity of the person(s) responsible for the internal control functions, including for the periodic, permanent and compliance controls, as well as an up-to-date curriculum vitae;

e) the identity of any auditor that is not a statutory auditor pursuant to Directive 2006/43/EC;

f) the composition of the management body and, if applicable, any other oversight body or committee;

g) a description of the way outsourced functions are monitored and controlled so as to avoid an impairment in the quality of the applicant's internal controls;

h) a description of the way any agents and branches are monitored and controlled within the framework of the applicant's internal controls;

i) where the applicant is the subsidiary of a regulated entity in another EU Member State, a description of the group governance.

Guideline 7: Procedure for monitoring, handling and following up on security incidents and security-related customer complaints

7.1. The applicant should provide a description of the procedure in place to monitor, handle and follow up on security incidents and security-related customer complaints to be provided by the applicant, which should contain:

a) organisational measures and tools for the prevention of fraud;

b) details of the individuals and bodies responsible for assisting customers in cases of fraud, technical issues and/or claim management;

c) reporting lines in cases of fraud;

d) the contact point for customers, including a name and email address;

e) the procedures for the reporting of incidents, including the communication of these reports to internal or external bodies, including the notification of major incidents to national competent authorities under Article 96 of PSD2 and in line with EBA guidelines on incident reporting under the referred Article.

f) the monitoring tools used and the follow-up measures and procedures in place to mitigate security risks.

Guideline 8: Process in place to file, monitor, track and restrict access to sensitive payment data

8.1. The applicant should provide a description of the process in place to file, monitor, track, and restrict access to sensitive payment data consisting of:

a) a description of the flow of data classified as sensitive payment data in the context of the AISP's business model;

b) the procedures in place to authorise access to the sensitive payment data;

c) a description of the monitoring tool;

d) the access right policy, detailing access to all relevant infrastructure components and systems, including databases and back-up infrastructures;

e) a description of how the collected data are filed;

f) the expected internal and/or external use of the collected data, including by counterparties;

g) the IT system and technical security measures that have been implemented, including encryption and/or tokenisation;

h) identification of the individual(s), bodies and/or committee(s) with access to the sensitive payment data;

i) an explanation of how breaches will be detected and addressed;

j) an annual internal control programme in relation to the safety of the IT systems.

Guideline 9: Business continuity arrangements

9.1. The applicant should provide a description of the business continuity arrangements consisting of the following information:

a) a business impact analysis, including the business processes and recovery objectives, such as recovery time objectives, recovery point objectives and protected assets;

b) the identification of the back-up site, access to IT infrastructure, and the key software and data to recover from a disaster or disruption;

c) an explanation of how the applicant will deal with significant continuity events and disruptions, such as the failure of key systems; the loss of key data; the inaccessibility of the premises; and the loss of key persons;

d) the frequency with which the applicant intends to test the business continuity and disaster recovery plans, including how the results of the testing will be recorded.

Guideline 10: Security policy document

10.1. The applicant should provide a security policy document containing the following information:

a) a detailed risk assessment of the payment service(s) the applicant intends to provide, which should include risks of fraud and the security control and mitigation measures taken to adequately protect payment service users against the risks identified;

b) a description of the IT systems, which should include:

i. the architecture of the systems and their network elements;

ii. the business IT systems supporting the business activities provided, such as the applicant's website, the risk and fraud management engine, and customer accounting;

iii. the support IT systems used for the organisation and administration of the AISP, such as accounting, legal reporting systems, staff management, customer relationship management, e-mail servers and internal file servers;

iv. information on whether or not those systems are already used by the AISP or its group, and the estimated date of implementation, if applicable;

c) the type of authorised connections from outside, such as with partners, service providers, entities of the group and employees working remotely, including the rationale for such connections;

d) for each of the connections listed under point c), the logical security measures and mechanisms in place, specifying the control the payment institution will have over such access as well as the nature and frequency of each control, such as technical versus organisational; preventative versus detective; real-time monitoring versus regular reviews, such as the use of an active directory separate from the group, the opening/closing of communication lines, security equipment configuration, generation of keys or client authentication certificates, system monitoring, authentication, confidentiality of communication, intrusion detection, antivirus systems and logs;

e) the logical security measures and mechanisms that govern the internal access to IT systems, which should include:

   i. the technical and organisational nature and frequency of each measure, such as whether it is preventative or detective and whether or not it is carried out in real time;

   ii. how the issue of client environment segregation is dealt with in cases where the applicant's IT resources are shared;

f) the physical security measures and mechanisms of the premises and the data centre of the applicant, such as access controls and environmental security;

g) the security of the payment processes, which should include:

   i. the customer authentication procedure used for both consultative and transactional access;

   ii. an explanation of how safe delivery to the legitimate payment service user and the integrity of authentication factors, such as hardware tokens and mobile applications, are ensured, at the time of both initial enrolment and renewal;

   iii. a description of the systems and procedures that the applicant has in place for transaction analysis and the identification of suspicious or unusual transactions.

h) a detailed risk assessment in relation to its payment services, including fraud, with a link to the control and mitigation measures explained in the application file, demonstrating that the risks are addressed;

i) a list of the main written procedures in relation to the applicant's IT systems or, for procedures that have not yet been formalised, an estimated date for their finalisation.

Guideline 11: Identity and suitability assessment of directors and persons responsible for the management of the account information service provider

11.1. For the purposes of the identity and suitability assessment of directors and persons responsible for the management of the account information service provider, the applicant should provide the following information:

a) personal details, which should include:

i. the full name, gender, place and date of birth, address and nationality, and personal identification number or copy of ID card or equivalent;

ii. details of the position for which the assessment is sought, and whether or not the management body position is executive or non-executive; this should also include the following details:

- the letter of appointment, contract, offer of employment or relevant drafts, as applicable;
- the planned start date and duration of the mandate;
- a description of the individual's key duties and responsibilities;

b) where applicable, information on the suitability assessment carried out by the applicant, which should include details of the result of any assessment of the suitability of the individual performed by the institution, such as relevant board minutes or suitability assessment reports or other documents;

c) evidence of knowledge, skills and experience, which should include a curriculum vitae containing details of education and professional experience, including academic qualifications, other relevant training, the name and nature of all organisations for which the individual works or has worked, and the nature and duration of the functions performed, in particular highlighting any activities within the scope of the position sought;

d) evidence of reputation, honesty and integrity, which should include:

i. criminal records and relevant information on criminal investigations and proceedings, relevant civil and administrative cases, and disciplinary actions, including disqualification as a company director, bankruptcy, insolvency and similar procedures, notably through an official certificate or any objectively

reliable source of information concerning the absence of criminal conviction, investigations and proceedings, such as third-party investigations, testimonies made by a lawyer or a notary established in the European Union;

ii. a statement as to whether or not criminal proceedings are pending or the person or any organisation managed by him or her has been involved as a debtor in insolvency proceedings or comparable proceedings;

iii. information concerning the following:

- investigations, enforcement proceedings or sanctions by a supervisory authority that the individual has been directly or indirectly involved in;
- refusal of registration, authorisation, membership or licence to carry out a trade, business or profession; the withdrawal, revocation or termination of registration, authorisation, membership or licence; or expulsion by a regulatory or government body or by a professional body or association;
- dismissal from employment or a position of trust, fiduciary relationship or similar situation, or having been asked to resign from employment in such a position, excluding redundancies;
- whether or not an assessment of reputation of the individual as an acquirer or a person who directs the business of an institution has already been conducted by another competent authority, including the identity of that authority, the date of the assessment and evidence of the outcome of this assessment, and the consent of the individual, where required, to seek and process such information and use the provided information for the suitability assessment;
- whether or not any previous assessment of the individual, on authority from another, non-financial sector, has already been conducted, including the identity of that authority and the evidence of the outcome of this assessment.

Guideline 12: Professional indemnity insurance or a comparable guarantee

12.1. As evidence of a professional indemnity insurance or comparable guarantee that is compliant with the EBA Guidelines on Professional Indemnity Insurance (EBA/GL/2017/08) and Articles 5(2)and 5(3) of PSD2 the applicant should provide the following information:

a) an insurance contract or other equivalent document confirming the existence of professional indemnity insurance or a comparable guarantee, with a cover amount that

is compliant with the referred EBA Guideline showing the coverage of the relevant liabilities;

b) documentation of how the applicant has calculated the minimum amount in a way that is compliant with the referred EBA Guidelines, including all applicable components of the formula specified therein.

4.3. Guidelines on the information requirements from applicants for authorisation as electronic money institutions

Guideline 1: General principles

1.1 This set of guidelines applies to applicants for authorisation as electronic money institutions (EMIs).This refers to applicants that intend to provide e-money services and, if applicable, any payment service(s) referred to in points 1-8 of Annex I to PSD2. Applicants that intend to provide only payment services referred to in points 1-7 of Annex I to PSD2 or service 8 referred to in this Annex in combination with other service(s) referred to in points 1-7 without providing e-money services should refer to the specific set of guidelines on the information required from applicants for authorisation as payment institutions (PIs) set out in section 4.1. Applicants that intend to provide only the payment service referred to in point 8 of Annex I to PSD2 without providing e-money services should refer to the guidelines on the information required from applicants for registration for the provision of only service 8 of Annex I PSD2 set out in section 4.2.

1.2 The information provided by applicants should be true, complete, accurate and up to date. All applicants should comply with all the provisions in the set of guidelines that applies to them. The level of detail should be proportionate to the applicant's size and internal organisation, and to the nature, scope, complexity and riskiness of the particular service(s) that the applicant intends to provide. In any event, in accordance with Directive (EU) 2015/2366, the directors and the persons responsible for the management of the electronic money institution are of good repute and possess appropriate knowledge and experience to perform payment services, regardless of the institution's size, internal organisation and the nature, scope and complexity of its activities and the duties and responsibilities of the specific position.

1.3 When submitting the information required, the applicant should avoid making references to specific sections of internal procedures/documents. Instead, the applicant should extract the relevant sections and provide these to the competent authority.

1.4 Should the competent authorities (CAs) require clarifications on the information that has been submitted, the applicant should provide such clarification without delay.

1.5 All data requested under these guidelines for authorisation as EMIs are needed for the assessment of the application and will be treated by the competent authority in accordance with the professional secrecy obligations set out in PSD2, without prejudice to applicable Union law and national requirements and procedures on the exercise of the right to access, rectify, cancel or oppose.

Guideline 2: Identification details

2.1 The identification details to be provided by the applicant should contain the following information:

a) the applicant's corporate name and, if different, trade name;

b) an indication of whether the applicant is already incorporated or in the process of incorporation;

c) the applicant's national identification number, if applicable;

d) the applicant's legal status and (draft) articles of association and/or constitutional documents evidencing the applicant's legal status;

e) the address of the applicant's head office and registered office;

f) the applicant's electronic address and website, if available;

g) the name(s) of the person(s) in charge of dealing with the application file and authorisation procedure, and their contact details;

h) an indication of whether or not the applicant has ever been, or is currently being, regulated by a competent authority in the financial services sector;

i) any trade association(s), in relation to the provision of e-money services and/or payment services, that the applicant plans to join, where applicable;

j) the register certificate of incorporation or, if applicable, negative certificate of a mercantile register that certifies that the name applied by the company is available;

k) evidence of the payment of any fees or of the deposit of funds to file an application for authorisation as an electronic money institution, where applicable under national law.

Guideline 3: Programme of operations

3.1 The programme of operations to be provided by the applicant should contain the following information:

a) an indication of the e-money services the applicant intends to provide: issuance, redemption, distribution;

b) if applicable, a step-by-step description of the type of payment services envisaged, including an explanation of how the activities and the operations that will be provided are identified by the applicant as fitting into any of the legal categories of payment services listed in Annex I to PSD2, and an indication of whether these payment services would be provided in addition to electronic money services or whether they are linked to the issuance of electronic money;

c) a declaration of whether the applicant will at any point enter or not into possession of funds;

d) if applicable, a description of the execution of the different e-money services and, if applicable, payment services, detailing all parties involved, for each e-money service and, if applicable, each payment service provided:

   i. a diagram of flow of funds;

   ii. settlement arrangements;

   iii. draft contracts between all the parties involved in the provision of payment services including those with payment card schemes, if applicable;

   iv. processing times;

e) a copy of the draft contract between the electronic money issuer and the electronic money holder and the draft framework contract, as defined in Article 4(21) of PSD2 if the applicant pretends to provide payment services in addition to e-money services;

f) the estimated number of different premises from which the applicant intends to provide the services, if applicable;

g) a description of any ancillary services to e-money services and, if applicable, to payment services;

h) when the applicant intends to provide payment services in addition to e-money services, a declaration of whether or not the applicant intends to grant credit and, if so, within which limits;

i) a declaration of whether or not the applicant plans to provide e-money services and, if applicable, payment services in other EU Member States or third countries after the granting of the licence;

j) an indication of whether or not the applicant intends, for the next three years, to provide or already provides business activities other than e-money services and, if applicable, payment services, as referred to in Article 11(5) of Directive (EU) 2015/2366, including a description of the type and expected volume of the activities;

k) the information specified in EBA Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366' (EBA/GL2017/08), where the applicant intends to provide services 7 and 8 (payment initiation services (PIS) and account information services (AIS)).

Guideline 4: Business plan

4.1. The business plan to be provided by the applicant should contain:

a) a marketing plan consisting of:

   i. an analysis of the company's competitive position in the e-money market and, if applicable, payment market segment concerned;

   ii. a description of the payment service users and electronic money holders, marketing materials and distribution channels;

b) certified annual accounts for the previous three years, if available, or a summary of the financial situation for those companies that have not yet produced annual accounts;

c) a forecast budget calculation for the first three financial years that demonstrates that the applicant is able to employ appropriate and proportionate systems, resources and procedures that allow the applicant to operate soundly; it should include:

   i. an income statement and balance-sheet forecast, including target scenarios and stress scenarios as well as their base assumptions, such as volume and value of transactions, number of clients, pricing, average amount per transaction, expected increase in profitability threshold;

   ii. explanations of the main lines of income and expenses, the financial debts and the capital assets;

   iii. a diagram and detailed breakdown of the estimated cash flows for the next three years;

d) information on own funds, including the amount and detailed breakdown of the composition of initial capital as set out in Article 57(a) and (b) of Directive 2006/48/EC;

e) information on, and calculation of, minimum own funds requirements in accordance with method D, as referred to in Article 5.3 of Directive (EU) 2009/110 (the second E-Money Directive (EMD2)), if the electronic money institution intends to provide e-money services only, or the method(s) referred to in Article 9 of Directive (EU) 2015/2366 (PSD2) as determined by the competent authority, if the applicant intends to provide payment services in addition to e-money services, including an annual projection of the breakdown of own funds for three years according to the method used and, If applicable, an annual projection of the own funds for three years according to the other methods used.

Guideline 5: Structural organisation

5.1. The applicant should provide a description of the structural organisation of its undertaking consisting of:

a) a detailed organisational chart, showing each division, department or similar structural separation, including the name of the person(s) responsible, in particular those in charge of internal control functions; the chart should be accompanied by a description of the functions and responsibilities of each division, department or similar structural separation;

b) an overall forecast of the staff numbers for the next three years;

c) a description of the relevant operational outsourcing arrangements consisting of:

   i. the identity and geographical location of the outsourcing provider;

   ii. the identity of the persons within the electronic money institution that are responsible for each of the outsourced activities;

   iii. a clear description of the outsourced activities and their main characteristics;

d) a copy of draft outsourcing agreements;

e) a description of the use of branches, agents and distributors, where applicable, including:

   i. a mapping of the off-site and on-site checks that the applicant intends to perform of branches, agents and distributors;

   ii. the IT systems, processes and infrastructure that are used by the applicant's agents and distributors to perform activities on behalf of the applicant;

iii. in the case of agents and distributors, the selection policy, monitoring procedures, agents' and distributor's training and, where available, the draft terms of engagement of agents and distributors;

f) an indication of the national and/or international payment system that the applicant will access, if applicable;

g) a list of all natural or legal persons that have close links with the applicant, indicating their identities and the nature of those links.

Guideline 6: Evidence of initial capital

6.1. For the evidence of initial capital to be provided by the applicant (of EUR 350 000), the applicant should submit the following documents:

a) for existing undertakings, an audited account statement or public register certifying the amount of capital of the applicant;

b) for undertakings in the process of being incorporated, a bank statement issued by a bank certifying that the funds are deposited in the applicant's bank account.

Guideline 7: Measures to safeguard the funds of electronic money users and/or payment service users

7.1. Where the applicant safeguards the electronic money users' and/or payment service users' funds through depositing funds in a separate account in a credit institution or through an investment in secure, liquid, low-risk assets, the description of the safeguarding measures should contain:

a) a description of the investment policy to ensure the assets chosen are liquid, secure and low risk, if applicable;

b) the number of persons that have access to the safeguarding account and their functions;

c) a description of the administration and reconciliation process for electronic money users and, if applicable, payment service users, against the claims of other creditors of the electronic money institution, in particular in the event of insolvency;

d) a copy of the draft contract with the credit institution;

e) an explicit declaration by the electronic money institution of compliance with Article 10 of PSD2.

7.2. Where the applicant safeguards the funds of the electronic money users and, if applicable, the payment service users through an insurance policy or comparable guarantee from an insurance company or credit institution, and unless the applicant intends to provide PIS only, the description of the safeguarding measures should contain the following:

a) a confirmation that the insurance policy or comparable guarantee from an insurance company or credit institution is from an entity that is not part of the same group of firms as the applicant;

b) details of the reconciliation process in place to ensure that the insurance policy or comparable guarantee is sufficient to meet the applicant's safeguarding obligations at all times;

c) duration and renewal of the coverage;

d) a copy of the (draft) insurance agreement or (draft) comparable guarantee.

Guideline 8: Governance arrangements and internal control mechanisms

8.1. The applicant should provide a description of the governance arrangement and internal control mechanisms consisting of:

a) a mapping of the risks identified by the applicant, including the type of risks and the procedures the applicant will put in place to assess and prevent such risks, in relation to e-money services and, if applicable, payment services;

b) the different procedures to carry out periodical and permanent controls, including the frequency and the human resources allocated;

c) the accounting procedures by the which the applicant will record and report its financial information;

d) the identity of the person(s) responsible for the internal control functions, including for periodic, permanent and compliance control, as well as an up-to-date curriculum vitae;

e) the identity of any auditor that is not a statutory auditor pursuant to Directive 2006/43/EC;

f) the composition of the management body and, if applicable, any other oversight body or committee;

g) a description of the way outsourced functions are monitored and controlled so as to avoid an impairment in the quality of the electronic money institution's internal controls;

h) a description of the way any agents, branches and distributors are monitored and controlled within the framework of the applicant's internal controls;

i) where the applicant is the subsidiary of a regulated entity in another EU Member State, a description of the group governance.

Guideline 9: Procedure for monitoring, handling and following up on security incidents and security-related customer complaints

9.1. The applicant should provide a description of the procedure in place to monitor, handle and follow up on security incidents and security-related customer complaints to be provided by the applicant, which should contain:

a) organisational measures and tools for the prevention of fraud;

b) details of the individuals and bodies responsible for assisting customers in cases of fraud, technical issues and/or claim management;

c) reporting lines in cases of fraud;

d) the contact point for customers, including a name and email address;

e) the procedures for the reporting of incidents, including the communication of these reports to internal or external bodies, including for applicants that intend to provide payment services in addition to e-money services, and the notification of major incidents to national competent authorities under Article 96 of PSD2 and in line with the EBA guidelines on incident reporting under the referred Article.

f) the monitoring tools used and the follow-up measures and procedures in place to mitigate security risks.

Guideline 10: Process for filing, monitoring, tracking and restricting access to sensitive payment data

10.1. The applicant should provide a description of the process in place to file, monitor, track and restrict access to sensitive payment data consisting of:

a) a description of the flows of data classified as sensitive payment data in the context of the electronic money institution's business model;

b) the procedures in place to authorise access to the sensitive payment data;

c) a description of the monitoring tool;

d) the access right policy, detailing access to all relevant infrastructure components and systems, including databases and back-up infrastructures;

e) a description of how the collected data are filed;

f) the expected internal and/or external use of the collected data, including by counterparties;

g) the IT system and technical security measures that have been implemented, including encryption and/or tokenisation;

h) identification of the individuals, bodies and/or committees with access to the sensitive payment data;

i) an explanation of how breaches will be detected and addressed;

j) an annual internal control programme in relation to the safety of the IT systems.

Guideline 11: Business continuity arrangements

11.1. The applicant should provide a description of the business continuity arrangements consisting of the following information:

a) a business impact analysis, including the business processes and recovery objectives, such as recovery time objectives, recovery point objectives and protected assets;

b) the identification of the back-up site and access to IT infrastructure, and the key software and data to recover from a disaster or disruption;

c) an explanation of how the applicant will deal with significant continuity events and disruptions, such as the failure of key systems; the loss of key data; the inaccessibility of the premises; and the loss of key persons;

d) the frequency with which the applicant intends to test the business continuity and disaster recovery plans, including how the results of the testing will be recorded;

e) a description of the mitigation measures to be adopted by the applicant, in cases of the termination of its payment services, ensuring the execution of pending payment transactions and the termination of existing contracts.

Guideline 12: The principles and definitions applicable to the collection of statistical data on performance, transactions and fraud.

12.1. The applicant should provide a description of the principles and definitions applicable to the collection of the statistical data on performance, transactions and fraud consisting of the following information:

a) the type of data that is collected, in relation to customers, type of payment service, channel, instrument, jurisdictions and currencies;

b) the scope of the collection, in terms of the activities and entities concerned, including branches, agents and distributors;

c) the means of collection;

d) the purpose of collection;

e) the frequency of collection;

f) supporting documents, such as a manual, that describe how the system works.

Guideline 13: Security policy document

13.1. The applicant should provide a security policy document in relation to its e-money service(s) and, where applicable, payment service(s) containing the following information:

a) a detailed risk assessment of the e-money service(s) and, where applicable, the payment service(s) the applicant intends to provide, which should include risks of fraud and the security control and mitigation measures taken to adequately protect e-money service users and, where applicable, payment service users against the risks identified;

b) a description of the IT systems, which should include:

i. the architecture of the systems and their network elements;

ii. the business IT systems supporting the business activities provided, such as the applicant's website, wallets, the payment engine, the risk and fraud management engine, and customer accounting;

iii. the support IT systems used for the organisation and administration of the electronic money institution, such as accounting, legal reporting systems, staff management, customer relationship management, e-mail servers, internal file servers;

iv. information on whether those systems are already used by the electronic money institution or its group, and the estimated date of implementation, if applicable;

c) the type of authorised connections from outside, such as with partners, service providers, entities of the group and employees working remotely, including the rationale for such connections;

d) for each of the connections listed under point c), the logical security measures and mechanisms in place, specifying the control the electronic money institution will have over such access as well as the nature and frequency of each control, such as technical versus organisational; preventative versus detective; and real-time monitoring versus regular reviews, such as the use of an active directory separate from the group, the opening/closing of communication lines, security equipment configuration, generation of keys or client authentication certificates, system monitoring, authentication, confidentiality of communication, intrusion detection, antivirus systems and logs;

e) the logical security measures and mechanisms that govern the internal access to IT systems, which should include:

i. the technical and organisational nature and frequency of each measure, such as whether it is preventative or detective and whether or not it is carried out in real time;

ii. how the issue of client environment segregation is dealt with in cases where the applicant's IT resources are shared;

f) the physical security measures and mechanisms of the premises and the data centre of the applicant, such as access controls and environmental security;

g) the security of the e-money and, where applicable, payment processes, which should include:

i. the customer authentication procedure used for both consultative and transactional access, and for all underlying payment instruments;

ii. an explanation of how safe delivery to the legitimate e-money services user and, where applicable, payment service user and the integrity of authentication factors, such as hardware tokens and mobile applications, are ensured, at the time of both initial enrolment and renewal;

iii. a description of the systems and procedures that the electronic money institution has in place for transaction analysis and the identification of suspicious or unusual transactions;

h) a detailed risk assessment in relation to its e-money services and, where applicable, its payment services, including fraud, with a link to the control and mitigation measures explained in the application file, demonstrating that the risks are addressed;

i) a list of the main written procedures in relation to the applicant's IT systems or, for procedures that have not yet been formalised, an estimated date for their finalisation.

Guideline 14: Internal control mechanisms to comply with obligations in relation to money laundering and terrorist financing (AML/CFT obligations)

14.1 The description of the internal control mechanisms that the applicant has established in order to comply, where applicable, with those obligations should contain the following information:

a) the applicant's assessment of the money laundering and terrorist financing risks associated with its business, including the risks associated with the applicant's customer base, the products and services provided, the distribution channels used and the geographic areas of operation;

b) the measures the applicant has or will put in place to mitigate the risks and comply with applicable anti-money laundering and counter terrorist financing obligations, including the applicant's risk assessment process, the policies and procedures to comply with customer due diligence requirements, and the policies and procedures to detect and report suspicious transactions or activities;

c) the systems and controls the applicant has or will put in place to ensure that its branches, agents and distributors comply with applicable anti-money laundering and terrorist financing requirements, including, in cases where the agent, distributor or branch is located in another Member State;

d) arrangements the applicant has or will put in place to ensure that staff, agents and distributors are appropriately trained in anti-money laundering and counter terrorist financing matters;

e) the identity of the person in charge of ensuring the applicant's compliance with anti-money laundering and counter-terrorism obligations, and evidence that their anti-money laundering and counter-terrorism expertise is sufficient to enable them to fulfil this role effectively;

f) the systems and controls the applicant has or will put in place to ensure their anti-money laundering and counter terrorist financing policies and procedures remain up to date, effective and relevant;

g) the systems and controls the applicant has or will put in place to ensure that the agents and distributors do not expose the applicant to increased money laundering and terrorist financing risk;

h) the anti-money laundering and counter-terrorism manual for the staff of the applicant.

Guideline 15: Identity and suitability assessment of persons with qualified holdings in the applicant

15.1 For the purposes of the identity and evidence of the suitability of persons with qualifying holdings in the applicant electronic money institution, without prejudice to the assessment in accordance with the criteria, as relevant, introduced with Directive 2007/44/EC and specified in the joint guidelines for the prudential assessment of acquisitions of qualifying holdings (EBA/GL/2017/08), the applicant should submit the following information:

a) a description of the group to which the applicant belongs and an indication of the parent undertaking, where applicable;

b) a chart setting out the shareholder structure of the applicant, including:

i. the name and the percentage holding (capital/voting right) of each person that has or will have a direct holding in the share capital of the applicant, identifying those that are considered as qualifying holders and the reason for such qualifications;

ii. the name and the percentage holding (capital/voting rights) of each person that has or will have an indirect holding in the share capital of the applicant, identifying those that are considered as indirect qualifying holders and the reason for such qualification;

c) a list of the names of all persons and other entities that have or, in the case of authorisation, will have qualifying holdings in the applicant's capital, indicating for each such person or entity:

i. the number and type of shares or other holdings subscribed or to be subscribed;

ii. the nominal value of such shares or other holdings.

15.2 Where a person who has or, in the case of authorisation, will have a qualifying holding in the applicant's capital is a natural person, the application should set out all of the following information relating to the identity and suitability of that person:

a) the person's name and name at birth, date and place of birth, citizenship (current and previous), identification number (where available) or passport number, address and a copy of an official identity document;

b) a detailed curriculum vitae stating the education and training, previous professional experience and any professional activities or other functions currently performed;

c) a statement, accompanied by supporting documents, containing the following information concerning the person:

   i. subject to national legislative requirements concerning the disclosure of spent convictions, any criminal conviction or proceedings where the person has been found against and which were not set aside;

   ii. any civil or administrative decisions in matters of relevance to the assessment or authorisation process where the person has been found against and any administrative sanctions or measures imposed as a consequence of a breach of laws or regulations (including disqualification as a company director), in each case which were not set aside and against which no appeal is pending or may be filed;

   iii. any bankruptcy, insolvency or similar procedures;

   iv. any pending criminal investigations;

   v. any civil or administrative investigations, enforcement proceedings, sanctions or other enforcement decisions against the person concerning matters that may be considered to be relevant to the authorisation to commence the activity of an electronic money institution or to the sound and prudent management of an electronic money institution;

   vi. where such documents can be obtained, an official certificate or any other equivalent document evidencing whether any of the events set out in sub-paragraphs (i)-(v) has occurred in respect of the relevant person;

   vii. any refusal of registration, authorisation, membership or licence to carry out trade, business or a profession;

   viii. any withdrawal, revocation or termination of a registration, authorisation, membership or licence to carry out trade, business or a profession;

   ix. any expulsion by an authority or public sector entity in the financial services sector or by a professional body or association;

x. any position of responsibility with an entity subject to any criminal conviction or proceedings, administrative investigations, sanctions or other enforcement decisions for conduct failings, including in respect of fraud, dishonesty, corruption, money laundering, terrorist financing or other financial crime, or of failure to put in place adequate policies and procedures to prevent such events, held at the time when the alleged conduct occurred, together with details of such occurrences and of the person's involvement, if any, in them;

xi. any dismissal from employment or a position of trust, any removal from a fiduciary relationship (other than as a result of the relevant relationship coming to an end by passage of time) and any similar situation;

d) a list of undertakings that the person directs or controls and of which the applicant is aware of after due and careful enquiry; the percentage of control either direct or indirect in these companies; their status (whether or not they are active, dissolved, etc.); and a description of insolvency or similar procedures;

e) where an assessment of reputation of the person has already been conducted by a competent authority in the financial services sector, the identity of that authority and the outcome of the assessment;

f) the current financial position of the person, including details concerning sources of revenues, assets and liabilities, security interests and guarantees, whether granted or received;

g) a description of any links to politically exposed persons, as defined in Article 3(9) of Directive (EU) 2015/849[4].

15.3 Where a person or entity who has or, in the case of authorisation, will have a qualifying holding in the applicant's capital (including entities that are not a legal person and which hold or should hold the participation in their own name), the application should contain the following information relating to the identity and suitability of that legal person or entity:

a) name;

b) where the legal person or entity is registered in a central register, commercial register, companies register or similar register that has the same purposes of those aforementioned, a copy of the good standing, if possible, or otherwise a registration certificate;

[4] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L 141, 5.6.2015, p. 73).

c) the addresses of its registered office and, where different, of its head office, and principal place of business;

d) contact details;

e) corporate documents or, where the person or entity is registered in another Member State, a summary explanation of the main legal features of the legal form or the entity;

f) whether or not the legal person or entity has ever been or is regulated by a competent authority in the financial services sector or other government body;

g) where such documents can be obtained, an official certificate or any other equivalent document evidencing the information set out in paragraphs (a) to (e) issued by the relevant competent authority;

h) the information referred to in Guideline 15(2)(c), 15(2)(d), 15(2)(e),15(2)(f) and 15(2)(g) a in relation to the legal person or entity;

i) a list containing details of each person who effectively directs the business of the legal person or entity, including their name, date and place of birth, address, their national identification number, where available, and detailed curriculum vitae (stating relevant education and training, previous professional experience, any professional activities or other relevant functions currently performed), together with the information referred to in Guideline 15(2)(c) and 15(2)(d) in respect of each such person;

j) the shareholding structure of the legal person, including at least their name, date and place of birth, address and, where available, personal identification number or registration number and the respective share of capital and voting rights of direct or indirect shareholders or members and beneficial owners, as defined in Article 3(6) of Directive (EU) 2015/849;

k) a description of the regulated financial group of which applicant is a part, or may become a part, indicating the parent undertaking and the credit, insurance and security entities within the group; the name of their competent authorities (on an individual or consolidated basis); and

l) annual financial statements, at the individual and, where applicable, the consolidated and sub-consolidated group levels, for the last three financial years, where the legal person or entity has been in operation for that period (or, if less than three years, the period for which the legal person or entity has been in operation and financial statements were prepared), approved by the statutory auditor or audit firm within the

meaning of Directive 2006/43/EC[5], where applicable, including each of the following items:

i. the balance sheet;

ii. the profit-and-loss accounts or income statement;

iii. the annual reports and financial annexes and any other documents registered with the relevant registry or competent authority of the legal person;

m) where the legal person has not been operating for a sufficient period to be required to prepare financial statements for the three financial years immediately prior to the date of the application, the application shall set out the existing financial statements (if any);

n) where the legal person or entity has its head office in a third country, general information on the regulatory regime of that third country as applicable to the legal person or entity, including information on the extent to which the third country's anti-money laundering and counter-terrorist financing regime is consistent with the Financial Action Task Force Recommendations;

o) for entities that do not have legal personality such as a collective investment undertaking, a sovereign wealth fund or a trust, the application shall set out the following information:

i. the identity of the persons who manage assets and of the persons who are beneficiaries or subscribers, unit holders controlling the collective investment undertaking or having a holding enabling them to prevent the taking of decisions by the collective investment undertaking;

ii. a copy of the document establishing and governing the entity including the investment policy and any restrictions on investment applicable to the entity.

15.4 The application shall set out all of the following information for each natural or legal person or entity who has or, in the case of authorisation, will have a qualifying holding in the capital of the applicant should contain the following:

a) details of that person's or entity's financial or business reasons for owning that holding and the person's or the entity's strategy regarding the holding, including the period for which the person or the entity intends to hold the holding and any intention to increase, reduce or maintain the level of the holding in the foreseeable future;

[5] Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87-107).

b) details of the person's or entity's intentions in respect of the applicant and of the influence the person or the entity intends to exercise over the applicant, including in respect of the dividend policy, the strategic development and the allocation of resources of the applicant, whether or not it intends to act as an active minority shareholder and the rationale for such intention;

c) information on the person's or the entity's willingness to support the applicant with additional own funds if needed for the development of its activities or in the case of financial difficulties;

d) the content of any intended shareholder's or member's agreements with other shareholders or members in relation to the applicant;

e) an analysis as to whether or not the qualifying holding will impact in any way, including as a result of the person's close links to the applicant, on the ability of the applicant to provide timely and accurate information to the competent authorities;

f) the identity of each member of the management body or of senior management who will direct the business of the applicant and will have been appointed by, or following a nomination from, such shareholders or members, together with, to the extent not already provided, the information set out in Guideline 16 below.

15.5 The application should set out a detailed explanation of the specific sources of funding for the participation of each person or entity having a qualifying holding in the applicant's capital, which should include:

a) details on the use of private financial resources, including their availability and (so as to ensure that the competent authority is satisfied that the activity that generated the funds is legitimate) source;

b) details on access to financial markets, including details of financial instruments to be issued;

c) information on the use of borrowed funds, including the name of the lenders and details of the facilities granted, such as maturities, terms, security interests and guarantees, as well as information on the source of revenue to be used to repay such borrowings; where the lender is not a credit institution or a financial institution authorised to grant credit, the applicant should provide to the competent authorities information on the origin of the borrowed funds;

d) information on any financial arrangement with other persons who are shareholders or members of the applicant.

Guideline 16: Identity and suitability assessment of directors and persons responsible for the management of the electronic money institution

16.1 For the purposes of the identity and suitability assessment of directors and persons responsible for the management of the electronic money institution, the applicant should provide the following information:

a) Personal details including:

i. their full name, gender, place and date of birth, address and nationality, and personal identification number or copy of ID card or equivalent.

ii. details of the position for which the assessment is sought, whether or not the management body position is executive or non-executive. This should also include the following details:

- the letter of appointment, contract, offer of employment or relevant drafts, as applicable;
- the planned start date and duration of the mandate;
- a description of the individual's key duties and responsibilities.

b) where applicable, information on the suitability assessment carried out by the applicant which should include details of the result of any assessment of the suitability of the individual performed by the institution, such as relevant board minutes or suitability assessment reports or other documents;

c) evidence of knowledge, skills and experience, which should include a curriculum vitae containing details of education and professional experience, including academic qualifications, other relevant training, the name and nature of all organisations for which the individual works or has worked, and the nature and duration of the functions performed, in particular highlighting any activities within the scope of the position sought;

d) evidence of reputation, honesty and integrity, which should include:

i. criminal records and relevant information on criminal investigations and proceedings, relevant civil and administrative cases, and disciplinary actions, including disqualification as a company director, bankruptcy, insolvency and similar procedures, notably through an official certificate or any objectively reliable source of information concerning the absence of criminal conviction, investigations and proceedings, such as third-party investigations, testimonies made by a lawyer or a notary established in the European Union;

ii. a statement as to whether criminal proceedings are pending or the person or any organisation managed by him or her has been involved as a debtor in insolvency proceedings or comparable proceedings;

iii. information concerning the following :

- investigations, enforcement proceedings or sanctions by a supervisory authority that the individual has been directly or indirectly involved in;
- refusal of registration, authorisation, membership or licence to carry out a trade, business or profession; the withdrawal, revocation or termination of registration, authorisation, membership or licence; or expulsion by a regulatory or government body or by a professional body or association;
- dismissal from employment or a position of trust, fiduciary relationship or similar situation, or having been asked to resign from employment in such a position, excluding redundancies;
- whether or not an assessment of reputation of the individual as an acquirer or a person who directs the business of an institution has already been conducted by another competent authority, including the identity of that authority, the date of the assessment and evidence of the outcome of this assessment, and the consent of the individual where required to seek such information to be able to process and use the provided information for the suitability assessment;
- whether or not any previous assessment of the individual, on authority from another, non-financial sector, has already been conducted, including the identity of that authority and evidence of the outcome of such an assessment.

Guideline 17: Identity of statutory auditors and audit firms

The identity of statutory auditors and audit firms as defined in Directive 2006/43/EC to be provided by the applicant, where relevant, should contain the names, addresses and contact details of auditors.

Guideline 18: Professional indemnity insurance or a comparable guarantee for payment initiation services and account information services

As evidence of a professional indemnity insurance or comparable guarantee that is compliant with EBA Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional insurance or other comparable guarantee (EBA/GL/2017/08) and Article 5(2) and

5(3) of PSD2, the applicant for authorisation as electronic money institutions that, in addition to e-money services, intends to provide PIS or AIS, should provide the following information:

a) an insurance contract or other equivalent document confirming the existence of the professional indemnity insurance or comparable guarantee, with a cover amount that is compliant with the referred EBA Guidelines, showing the coverage of the respective liabilities;

b) documentation of how the applicant has calculated the minimum amount in a way that is compliant with the referred EBA Guidelines (EBA/GL/2017/08), including all applicable components of the formula specified therein.

4.4. Guidelines regarding the assessment of completeness of the application

Guideline 1: Assessment of the completeness of the application

1.1. An application should be deemed to be complete for the purpose of Article 12 of Directive (EU) 2015/2366 if it contains all the information needed by the competent authorities in order to assess the application in accordance with these guidelines and with Article 5 of Directive (EU) 2015/2366.

1.2. Where the information provided in the application is assessed to be incomplete, the competent authority should send, in paper format or by electronic means, a request to the applicant, indicating in a clear way what information is missing, and should provide to the applicant the opportunity to submit the missing information.

1.3. Upon an application being assessed as complete, the competent authority should inform the applicant of that fact, together with the date of receipt of the complete application or, as the case may be, the date of receipt of the information that completed the application.

1.4. In any case, the competent authority may require the applicant to provide clarification on the information for the purposes of assessing the application.

1.5. Where an application contains information, or relies on information held by the competent authorities, which is no longer true, accurate or complete, an update to the application should be provided to the competent authorities without delay. The update should identify the information concerned, its location within the original application, the reason for the information no longer being true, accurate or complete, the updated information and confirmation that the rest of the information in the application remains true, accurate and complete.