To the Receipt stamp

Financial Market Authority Liechtenstein (FMA)

*Please tick the applicable options, add other remarks and references as required and enclose the signed checklist as an attachment with the written application for the issuing of a licence as an e-money institution in accordance with the Liechtenstein E-Money Act of 17 March 2011 (*E-Geldgesetz vom 17. März 2011, EGG *– hereinafter referred to as the “EMA”) and the Liechtenstein E-Money Ordinance of 17 June 2025 (*E-Geldverordnung vom 17. June 2025, EGV*– hereinafter referred to as the “EMO”), making sure to number the respective enclosures. The application, including the enclosures, must be submitted in writing* ***and*** *electronically (PDF format). In the case of notarised (and possibly apostilled) documents, a corresponding note must be applied in the electronic document upon it being submitted electronically if this is not already visible in the electronic document.*

**Details on the identity of the applicant**

*a) Details if the notifier is an individual:*

|  |  |  |
| --- | --- | --- |
| *Last name*  | *Last name at birth*  | *First name(s)*  |
| *Date of birth*  | *Place of birth*  | *Country of birth*  | *Nationality (nationalities)*  |
| *Address of principal place of residence* | *Street*  | *Number*  |
| *Postcode*  | *Town or city*  |

*b) Details if the notifier is a legal entity:*

|  |  |
| --- | --- |
| *Company name*  | *Legal form*  |
| *Registered office*  | *Postcode*  | *Country of registered office*  |
| *Address of main branch* | *Street*  | *Number*  |
| *Postcode*  | *Town or city*  | *Country*  |

*c) Authorised recipient (if appointed):*

|  |  |  |
| --- | --- | --- |
| *Last name (or name of entity)*  | *First name(s) (or legal form)*  | *Date of birth (if applicable)*  |
| *Address of principal place of residence (or main branch)* | *Street*  | *Number*  |
| *Postcode*  | *Town or city*  |

*d) Authorised legal representative, provided the notifier is represented:*

|  |  |  |
| --- | --- | --- |
| *Last name (or name of entity)*  | *First name(s) (or legal form)*  | *Date of birth (if applicable)*  |
| *Address of principal place of residence (or main branch)* | *Street*  | *Number*  |
| *Postcode*  | *Town or city*  |

*e) Contact person*[[1]](#footnote-1) *(for enquiries):*

|  |  |
| --- | --- |
| *Last name*   | *First name(s)*   |
| *Address* | *Street*  | *Number*  |
| *Postcode*   | *Town or city*   |
| *Telephone number*  | *E-mail address*  |

**Information to be enclosed**

Details on the information to be included in the enclosures can be found in the FMA Guidelines 2018/18 and in Article 7 in conjunction with Article 3 of the European Banking Authority (EBA) 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 (EBA/GL/2017/09).

The enclosures to be submitted must bear the relevant, continuous enclosure number in accordance with the following table. In the case of multi-page enclosures, the exact reference must always be provided.

In specific cases, if information only is applicable to a limited extent or in part, the original of a corresponding signed and dated declaration from the applicant must be enclosed under all circumstances. If it is not possible to provide a declaration for one of the named points, written justification must also be submitted to the FMA.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **EBA****Guidelines****2017/09** | **Section** | **Letter** | **Description** | **Enclosure No.** | **Enclosed** | **Not enclosed** | **Not applicable** | **Remarks** | **Field reserved for the FMA** |
| *Identification details* | 2.1 | a | The applicant’s corporate/company name and, if different, its trade name |   | [ ]  | [ ]  | [ ]  |   |   |
| b | Details on whether the applicant is already a registered company or is in the process of incorporation |   | [ ]  | [ ]  | [ ]  |   |   |
| c | The applicant’s national identification number, if applicable |   | [ ]  | [ ]  | [ ]  |   |   |
| d | The applicant’s legal form and (draft) articles of association and/or constitutional documents evidencing the applicant’s legal form |   | [ ]  | [ ]  | [ ]  |   |   |
| 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 and authorisation procedure as well as their contact details |   | [ ]  | [ ]  | [ ]  |   |   |
| h | Details on whether or not the applicant has ever been, or is currently, subject to regulation/supervision by a competent authority in the financial services sector |   | [ ]  | [ ]  | [ ]  |   |   |
| i | Where applicable, details on the industry association or associations relating to the provision of e-money services and/or payment services that the applicant intends to join |   | [ ]  | [ ]  | [ ]  |   |   |
| j | Evidence of entry in the Commercial Register or, where applicable, a negative certificate of a Commercial Register that certifies that the name used 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 e-money institution |    | [ ]  | [ ]  | [ ]  |    |   |
| *Business model* | 3.1 | a | Details on the nature of the e-money services that the applicant intends to provide: issue, distribution, redemption |   | [ ]  | [ ]  | [ ]  |   |   |
| b | A step-by-step description of the nature of the payment services envisaged, including an explanation of how the planned activities and procedures are identified by the applicant as fitting into any of the legal categories of payment services listed in Annex 1 of the second edition of the Payment Services Directive (PSD2), whether these payment services will be offered in addition to the e-money services, and whether they are related to the issuing of e-money |   | [ ]  | [ ]  | [ ]  |   |   |
| c | A declaration of whether the applicant will, at any time, enter into the possession of funds |   | [ ]  | [ ]  | [ ]  |   |   |
| d | Where applicable, a description of the execution of the various aspects of the e-money services and, as appropriate, details of all parties involved in each individual aspect of the e-money services provided and, if required, the payment services, including:1. A diagram of cash flows
2. Payment settlement arrangements
3. Draft agreements between all the parties involved in the provision of payment services, including, where applicable, those with card payment procedures/payment card systems
4. Processing/lead times
 |   | [ ]  | [ ]  | [ ]  |   |   |
| e | A copy of the agreement between the e-money issuer and the e-money holder as well as the draft framework agreement as defined in Article 4(21) PSD2 if the applicant intends to provide payment services in addition to the e-money services |   | [ ]  | [ ]  | [ ]  |   |   |
| f | Where applicable, the estimated number of operating sites from which the applicant intends to provide its services |   | [ ]  | [ ]  | [ ]  |   |   |
| g | A description of ancillary services to the e-money services and, where applicable, the payment services |   | [ ]  | [ ]  | [ ]  |   |   |
| h | If the applicant intends to provide payment services in addition to the e-money services, a declaration of whether and, if so, within which limits the applicant intends to grant loans |   | [ ]  | [ ]  | [ ]  |   |   |
| i | A declaration of whether the applicant intends to provide the e-money services and, where applicable, payment services in EU Member States or third countries after the granting of the licence |   | [ ]  | [ ]  | [ ]  |   |   |
| j | Details on whether the applicant intends to undertake within the next three years or already undertakes other commercial activities in addition to the e-money services and, where applicable, payment services as per Article 11(5) of Directive (EU) 2015/2366, including a description of the type and estimated scope of the activities |  | [ ]  | [ ]  | [ ]  |    |   |
| *Business plan* | 4.1 | a | A marketing plan consisting of:1. An analysis of the company’s competitive position in the relevant segment of the e-money market and, where applicable, the payment services market
2. A description of the payment services users and e-money holders, marketing materials and distribution channels
 |   | [ ]  | [ ]  | [ ]  |   |   |
| b | Audited annual financial statements for the past three years (if available) or a summary of the financial situation for those companies that have not yet produced annual financial statements |   | [ ]  | [ ]  | [ ]  |   |   |
| c | A budget plan for the first three financial years that demonstrates that the applicant possesses adequate and appropriate systems, resources and procedures that allow it to properly perform its activities; this budget plan should include:1. An income statement/projected profit and loss statement and balance sheet forecast, including target scenarios and stress scenarios as well as their base assumptions, such as the volume and value of transactions, number of clients, pricing, average amount per transaction, expected increase in profitability threshold
2. Explanation of the main income and cost components, financial liabilities and capital assets
3. A diagram and detailed breakdown of the estimated cash flow statement for the next three years
 |   | [ ]  | [ ]  | [ ]  |   |   |
| d | Information on own funds, including the amount and a 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 capital requirements and their calculation in accordance with Article 10(5) EMA if the e-money institution only intends to provide e-money services, or in accordance with Article 10(4) EMA if the applicant also intends to provide payment services alongside its e-money services, including an annual projection of the breakdown of the own funds for three years according to the method used and, where applicable, an annual projection of the own funds for three years according to the other methods used |   | [ ]  | [ ]  | [ ]  |   |   |
| *Organisational structure* | 5.1 | a | A detailed organisational chart showing each division, department or similar structural separation, including the name(s) of the person(s) responsible, in particular those in charge of the internal control mechanisms; the organisational chart should be accompanied by a description of the functions and responsibilities of each division, department or comparable structural separation |   | [ ]  | [ ]  | [ ]  |   |   |
| b | An overall forecast of staff numbers for the next three years |   | [ ]  | [ ]  | [ ]  |   |   |
| c | A description of the relevant operational outsourcing agreements with the following details:1. Name and geographic location of the outsourcing company
2. Names of the persons within the e-money institution who are responsible for the individual outsourced activities
3. A clear description of the outsourced activities and their key characteristics
 |   | [ ]  | [ ]  | [ ]  |   |   |
| d | A copy of the draft outsourcing agreements |   | [ ]  | [ ]  | [ ]  |   |   |
| e | A description of the use of branches, agents and distributors, including, where applicable, the following details:1. An account of the on-site and off-site checks that the applicant intends to perform at branches, agents and distributors
2. The IT systems, processes and infrastructures used by the applicant’s agents and distributors to perform activities on behalf of the applicant
3. In the case of agents and distributors, the selection process, monitoring procedures and training measures of the agents and distributors as well as, where applicable, the draft contractual conditions of the agents and distributors
 |   | [ ]  | [ ]  | [ ]  |   |   |
| f | Where applicable, details on the national and/or international payment system to which the applicant will have access |   | [ ]  | [ ]  | [ ]  |   |   |
| g | A list of all individuals and legal entities that have close links with the applicant, including details of their identity and the nature of these links |  | [ ]  | [ ]  | [ ]  |  |   |
| *Evidence of* *initial capital* | 6.1 | a | **For existing companies:** audited accounts/a bank confirmation or an excerpt from a public register certifying the amount of capital of the applicant |   | [ ]  | [ ]  | [ ]  |   |   |
| b | **For companies in the process of being incorporated:** an account statement issued by a bank certifying that the capital has been deposited to the applicant’s bank account |   | [ ]  | [ ]  | [ ]  |  |   |
| *Measures for safeguarding of funds*  | ***If the applicant safeguards the funds of e-money users and/or payment services users by depositing the funds to a separate account at a bank or through an investment in secure liquid assets with a low level of risk, the description of the safeguarding measures should contain the following:*** |   | [ ]  | [ ]  | [ ]  |   |   |
| 7.1 | a | Where applicable, a description of the investment strategy/policy to ensure that the selected assets meet the criteria stipulated in the FMA Guidelines 2018/2[[2]](#footnote-2) |   | [ ]  | [ ]  | [ ]  |   |   |
| b | The number and functions of the persons with access to the fiduciary account |   | [ ]  | [ ]  | [ ]  |   |   |
| c | A description of the administration and account reconciliation process for e-money users and, where applicable, payment services users to ensure protection against the claims of other creditors of the e-money institution, in particular in the event of insolvency |   | [ ]  | [ ]  | [ ]  |   |   |
| d | A copy of the draft agreement with the bank |   | [ ]  | [ ]  | [ ]  |   |   |
| e | An explicit declaration from the e-money institution of compliance with Article 10 PSD2 |   | [ ]  | [ ]  | [ ]  |   |   |
| ***If the applicant safeguards the funds of e-money users and, where applicable, payment services users through an insurance policy or a comparable guarantee from an insurance company or bank and the applicant does not intend to exclusively provide payment initiation services, the description of the safeguarding measures should contain the following:*** |   | [ ]  | [ ]  | [ ]  |   |   |
| 7.2 | a | A confirmation that the insurance policy or comparable guarantee from an insurance company or a bank originates from a company that is not part of the same group of companies as the applicant |   | [ ]  | [ ]  | [ ]  |   |   |
| b | Details on the (account) reconciliation process in place to ensure that the insurance policy or comparable guarantee is sufficient to meet the safeguarding obligations of the applicant at all times |   | [ ]  | [ ]  | [ ]  |   |   |
| c | Duration and extension/renewal of the coverage |   | [ ]  | [ ]  | [ ]  |   |   |
| d | A copy of the (draft) insurance agreement or (draft) comparable guarantee |   | [ ]  | [ ]  | [ ]  |   |   |
| *Governance arrangements and internal control mechanisms* | 8.1 | a | An account of the risks identified by the applicant, including the nature of the risks and the procedures that the applicant will put in place to assess and prevent such risks in relation to the e-money services and, where applicable, payment services |   | [ ]  | [ ]  | [ ]  |   |   |
| b | The different procedures for the performance of regular and permanent controls, including details on the frequency of the controls and the human resources assigned for this purpose |   | [ ]  | [ ]  | [ ]  |   |   |
| c | The accounting standards on the basis of which the applicant will record and report its financial information |   | [ ]  | [ ]  | [ ]  |   |   |
| d | The identity or identities of and an up-to-date CV for the person(s) who is/are responsible for the internal control functions, including the regular and permanent performance of the controls and compliance therewith |   | [ ]  | [ ]  | [ ]  |   |   |
| e | The identity of auditors that are not classified as statutory auditors under Directive 2006/43/EC |   | [ ]  | [ ]  | [ ]  |   |   |
| f | The composition of the governing body and, where applicable, other supervisory bodies or committees |   | [ ]  | [ ]  | [ ]  |   |   |
| g | A description of how outsourced tasks are monitored and controlled so as to ensure the quality of the internal controls of the e-money institution is not adversely affected |   | [ ]  | [ ]  | [ ]  |   |   |
| h | A description of how agents, branches and distributors are monitored and controlled within the framework of the applicant’s internal controls |   | [ ]  | [ ]  | [ ]  |   |   |
| i | If the applicant is a subsidiary of a regulated company in an EU Member State, a description of the group governance |  | [ ]  | [ ]  | [ ]  |    |   |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Procedure for monitoring, handling and following up on security incidents and security-related client complaints* | 9.1 | a | Organisational measures and procedures for the prevention of fraud |   | [ ]  | [ ]  | [ ]  |   |   |
| b | Details of the individuals and bodies responsible for supporting clients in cases of fraud, technical issues and/or claim management |   | [ ]  | [ ]  | [ ]  |   |   |
| c | Reporting lines in cases of fraud |   | [ ]  | [ ]  | [ ]  |   |   |
| d | The contact point for clients, including a name and an e-mail 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 competent national authorities in accordance with Article 96 of the PSD2 and in line with the EBA Guidelines on incident reporting under the named article |   | [ ]  | [ ]  | [ ]  |   |   |
| f | The monitoring tools used and the follow-up measures and procedures in place to mitigate security risks |   | [ ]  | [ ]  | [ ]  |  |   |
| *Process for recording, monitoring, tracking and restricting access to sensitive payment data* | 10.1 | a | A description of the streams/flows of data classified as sensitive payment data in the context of the e-money institution’s business model |   | [ ]  | [ ]  | [ ]  |   |   |
| b | The procedures in place to authorise access to sensitive payment data |   | [ ]  | [ ]  | [ ]  |   |   |
| c | A description of the monitoring procedure |   | [ ]  | [ ]  | [ ]  |   |   |
| d | Guidelines/directives/procedures relating to access rights that govern access to all relevant infrastructure components and systems, including databases and back-up infrastructures |   | [ ]  | [ ]  | [ ]  |   |   |
| e | A description of how the collected data is recorded |   | [ ]  | [ ]  | [ ]  |   |   |
| f | Details on the expected internal and/or external use of the collected data, including by counterparties |   | [ ]  | [ ]  | [ ]  |   |   |
| g | The IT system and technical security measures that are used, including encryption and/or tokenisation |   | [ ]  | [ ]  | [ ]  |   |   |
| h | Identification of the roles (persons, bodies and/or committees) with access to sensitive payment data |   | [ ]  | [ ]  | [ ]  |   |   |
| i | An explanation of how breaches are recognised and rectified |   | [ ]  | [ ]  | [ ]  |   |   |
| j | An annual inspection plan for internal controls with respect to the security of IT systems |   | [ ]  | [ ]  | [ ]  |   |   |
| *Business continuity arrangements* | 11.1 | a | A business impact analysis, including the business processes and recovery objectives, such as recovery time and recovery point objectives (maximum tolerable data loss) as well as protected assets |   | [ ]  | [ ]  | [ ]  |   |   |
| b | The identification of the back-up site, access to IT infrastructure and the key software and data to recover in the event of a disaster or disruption |   | [ ]  | [ ]  | [ ]  |   |   |
| c | An explanation of how the applicant will deal with significant continuity events and disruptions, for example the failure of critical systems, the loss of key data, the inaccessibility of business premises and the loss of key personnel |   | [ ]  | [ ]  | [ ]  |   |   |
| d | The frequency with which the applicant intends to test the business continuity and disaster recovery plans, including details on how the results of this testing will be recorded |   | [ ]  | [ ]  | [ ]  |   |   |
| e | A description of the risk 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 agreements |    | [ ]  | [ ]  | [ ]  |   |   |
| *The principles and definitions applicable to the recording of statistical data on performance, transactions and cases of fraud* | 12.1 | a | The nature of the data that is recorded in relation to clients, the type of payment service, the payment channel, the payment instrument, jurisdictions and currencies |   | [ ]  | [ ]  | [ ]  |   |   |
| b | The scope of the recording with respect to the activities and companies concerned, including branches, agents and distributors |   | [ ]  | [ ]  | [ ]  |   |   |
| c | How the data is recorded |   | [ ]  | [ ]  | [ ]  |   |   |
| d | The purpose of the data recording |   | [ ]  | [ ]  | [ ]  |   |  |
| e | The frequency of data recording |   | [ ]  | [ ]  | [ ]  |   |  |
| f | Supporting documents, such as a manual that describes how the system works |    | [ ]  | [ ]  | [ ]  |   |   |
| *Security strategy document* | 13.1 | a | A detailed risk assessment of the e-money services and, where applicable, the payment services the applicant intends to provide, which should include the risks of fraud and the security control and risk mitigation measures in place to ensure the adequate protection of e-money users and, where applicable, payment services users against the risks identified |   | [ ]  | [ ]  | [ ]  |   |   |
| b | A description of the IT systems, which should include information on the following:1. The architecture of the systems and their network elements
2. The business IT systems supporting the business activities provided, such as the applicant’s website, wallets, payment engine, the risk and fraud management engine and a client overview
3. The support IT systems used for the organisation and administration of the e-money institution, such as accounting, legal reporting systems, HR management, client relationship management, e-mail servers and internal file servers
4. Details on whether these systems are already used by the e-money institution or its group as well as, where applicable, the estimated date of implementation
 |   | [ ]  | [ ]  | [ ]  |   |   |
| c | The type of authorised connections from outside, such as with partners, service providers, group companies and employees working remotely, including the reasons for such connections |   | [ ]  | [ ]  | [ ]  |   |   |
| d | For each of the connections listed under point c), the logical security measures and mechanisms in place, including details of the control the e-money institution will have over such access as well as the nature and frequency of the individual controls, such as technical versus organisational and preventative versus detective as well as real-time monitoring versus regular reviews, including the use of one of the active directories separate from the group, the opening/closing of communication lines, the configuration of security measures, the generation of keys or client authentication certificates, system monitoring, authentication, confidentiality of communication, the recognition of unauthorised access, antivirus systems and logs |   | [ ]  | [ ]  | [ ]  |   |   |
| e | The logical security measures and mechanisms that govern internal access to IT systems, which should include information on the following:1. 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
2. Details on how the issue of the segregation or protection of the client environment is dealt with in cases in which the applicant’s IT resources are shared
 |   | [ ]  | [ ]  | [ ]  |   |   |
| f | The physical security measures and mechanisms of the business premises and data centre of the applicant, such as access controls and environmental security |   | [ ]  | [ ]  | [ ]  |   |   |
| g | The security of the e-money and, where applicable, the payment processes, which should include:1. The client authentication procedure used for both consultative and transaction-related access as well as for all underlying payment instruments
2. An explanation of how safe delivery to the legitimate e-money user and, where applicable, payment services user and the integrity of authentication factors such as hardware tokens and mobile applications are ensured, both at the time of initial registration and upon renewal
3. A description of the systems and procedures that the e-money institution has set up for transaction analyses and the identification of suspicious or unusual processes/transactions
 |   | [ ]  | [ ]  | [ ]  |   |   |
| h | A detailed risk assessment in relation to its e-money services and, where applicable, payment services, including the risk of fraud, with a link to the control and risk mitigation measures explained in the application, demonstrating that these risks are addressed |   | [ ]  | [ ]  | [ ]  |   |   |
| i | A list of the most important written procedures (work instructions) in relation to the applicant’s IT systems or, for procedures that have not yet been formalised, the estimated date for their finalisation |   | [ ]  | [ ]  | [ ]  |   |   |
|  |  |  |  |  |  |  |  |  |  |
| *Internal control mechanisms to comply with requirements in relation to money laundering and terrorist financing*  | 14.1 | a | The applicant’s assessment with respect to the money laundering and terrorist financing risks associated with its business, including the risks associated with the applicant’s client base as well as its products and services, the distribution channels used and the geographic areas of operation |   | [ ]  | [ ]  | [ ]  |   |   |
| b | The measures that the applicant has or will put in place in order to meet the applicable requirements set out under due diligence legislation, for example Regulation (EU) No. 2015/847 on the prevention of money laundering and terrorist financing, including its risk assessment process, the guidelines and procedures for compliance with client due diligence requirements as well as the guidelines and procedures for the detection and reporting of suspicious processes/transactions or activities |   | [ ]  | [ ]  | [ ]  |   |   |
| c | The systems and controls that the applicant has or will put in place in order to ensure that its branches, agents and distributors comply with the applicable requirements for the prevention of money laundering and terrorist financing, including in cases in which the branch, agent or distributor is located in another EU Member State |   | [ ]  | [ ]  | [ ]  |   |   |
| d | Arrangements that the applicant has or will put in place in order to ensure that its personnel, agents and distributors are adequately trained in matters relating to the prevention of money laundering and terrorist financing |   | [ ]  | [ ]  | [ ]  |   |   |
| e | The identity of the person responsible for ensuring compliance with the requirements relating to the prevention of money laundering and terrorist financing and evidence that their specialist knowledge in this area is sufficient to enable them to fulfil this role effectively |   | [ ]  | [ ]  | [ ]  |   |   |
| f | The systems and controls that the applicant has or will put in place in order to ensure that its guidelines and procedures for the combating of money laundering and terrorist financing remain up to date, effective and relevant |   | [ ]  | [ ]  | [ ]  |   |   |
| g | The systems and controls that the applicant has or will put in place in order to ensure that its agents and distributors do not expose the applicant to increased money laundering and terrorist financing risk |   | [ ]  | [ ]  | [ ]  |   |   |
| h | The manual on the prevention of money laundering and terrorist financing for the applicant’s employees |    | [ ]  | [ ]  | [ ]  |    |   |
| *Identity and assessment of suitability of persons with a qualifying holding in the applicant* | 15.1 |   | See the [FMA Guidelines 2018/6](https://www.fma-li.li/fma-li/documents/rechtsgrundlagen/en/fma-guidance-2018-6.pdf)*[[3]](#footnote-3)* |   | [ ]  | [ ]  | [ ]  |   |   |
| *Identity and assessment of suitability of the directors and persons responsible**for the management of the e-money institution* | 16.1 |   | See [FMA Communication 2013/07](https://www.fma-li.li/fma-li/documents/rechtsgrundlagen/en/fma-communication-2013-7.pdf) |   | [ ]  | [x]  | [ ]  |   |   |
| *Identity of statutory auditors and audit firms* | 17 |  | The details on the identity of statutory auditors and audit firms as defined in Directive 2006/43/EC to be provided by the applicant should contain the name of the firm of auditors and, where applicable, the names, addresses and contact details of the auditors |   | [ ]  | [ ]  | [ ]  |   |   |

**Please note:**

If it is not possible to provide a declaration for one of the named points, written justification must be submitted to the FMA.

If a license for an e-money institution has already been reviewed by the FMA, any changes that have occurred since the last review must also be documented, with the provision of express confirmation that there are no further changes in addition to the stated changes. The completeness and accuracy of these details must be confirmed at the same time. In individual cases, the FMA will request the updating of documents that are already available.

By providing their signature, the undersigned confirm that the details provided in the checklist, including the enclosures and other information, are complete and accurate.

**Data protection:**

The FMA processes personal data exclusively in accordance with the general data processing principles of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) and in line with applicable data protection law.

Information regarding the processing of personal data, including details about the purpose of processing, the data controller and the rights of data subjects can be found in the FMA Privacy Policy: https://www.fma-li.li/en/fma/data-protection/fma-privacy-policy

……………………………., …………………….. ………………………………………………………….

(Place, date) (Name in block capitals and signature of the authorised representative)

| **Field reserved for the FMA** |
| --- |
| **Procedure** | **Date/remark** |
| Receipt of application for preliminary review |   |
| Request for additional documents |   |
| Receipt of definitive application  |   |
| R1:Result: [ ]  Approvable [ ]  Not approvable |   |
| R2: Result: [ ]  Approvable [ ]  Not approvable |   |
| Decision and communication of decision |   |
| CRM |   |
| Website/register/official journal |   |
| Internal information |   |

1. In addition to the address, please also provide, if known, the contact person and his or her contact details (telephone number, e-mail address). [↑](#footnote-ref-1)
2. These Guidelines will come into effect on 1 January 2019. [↑](#footnote-ref-2)
3. In accordance with the FMA Guidelines 2018/6, a separate form must be completed and submitted for each individual or legal entity with a qualifying holding. For details that are the same for all affected persons, references to the form of the person who provided the information or evidence are permitted. [↑](#footnote-ref-3)