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 to the written application for* ***registration as an account information service provider*** *under the Payment Services Act (ZDG) of 6 June 2019 and the Payment Services Ordinance (ZDV) of 17 September 2019, making sure to number the enclosures. The application, including the enclosures, must be submitted in writing* ***and*** *electronically (PDF format). In the case of notarised (and where applicable apostilled) documents, a note to that effect must be made in the electronic document upon it being submitted electronically if this is not already apparent from the electronic document.*

**Details on the identity of the applicant**

*a) Details if the applicant is a natural person*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Surname* | | *Surname at birth* | *Given 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 applicant is a legal person:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Company name* | | | *Legal form* | | |
| *Registered office* | | *Postcode* | *Country of registered office* | | |
| *Address of principal place of business* | *Street* | | | | *Number* |
| *Postcode* | *Town or city* | | *Country* | |

*c) Authorised recipient, where applicable:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Surname (or company name)* | | | *Given name(s) (or legal form)* | *Date of birth* |
| *Address of principal place of residence* | *Street* | | | *Number* |
| *Postcode* | *Town or city* | | |

*d) Authorised legal representative, where applicable:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Surname (or company name)* | | | *Given name(s) (or legal form)* | *Date of birth* |
| *Address of principal place of residence* | *Street* | | | *Number* |
| *Postcode* | *Town or city* | | |

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

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

**Information to be enclosed**

Details of the information to be enclosed can be found in [FMA Instruction 2019/8 – Licence to operate a payment institution](https://www.fma-li.li/files/list/fma-wegleitung-2019-8.pdf), Article 12 ZDG, and set 4.2 of the 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 proper enclosure number in accordance with the following table. If enclosures have several pages, the precise location in the enclosure must always be indicated.

Should specific information apply only to a limited extent or in part, the original of a signed and dated explanation to that effect by the applicant must always be enclosed. If no explanation can be provided for one or more of the enumerated points, a written justification must be submitted to the FMA.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **EBA**  **Guidelines**  **2017/09** | **Guideline** | **Point** | **Description** | **Enclosure no.** | **enclosed** | **not enclosed** | **not applicable** | **Comments** | **For FMA use only** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Identification details* | **If the applicant is a natural person, the identification details to be provided by the applicant must contain the following information:** | | |  |  |  |  |  |  |
| 2.1 | 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 |  |  |  |  |  |  |
| **If the applicant is a legal person, the identification details to be provided by the applicant must contain the following information:** | | |  |  |  |  |  |  |
| 2.2 | a | the applicant's corporate name and, if different, trade name |  |  |  |  |  |  |
| b | an indication of whether the applicant is already a registered undertaking or in process of formation |  |  |  |  |  |  |
| c | the applicant's national identification number, if applicable |  |  |  |  |  |  |
| d | the applicant's legal form and (draft) articles of association and/or formation 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 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 | evidence of entry in the Commercial Register or, if applicable, negative certificate of a commercial register that certifies that the name applied by the company is available |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Programme of operations* | 3.1 | 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(1)(25) ZDG |  |  |  |  |  |  |
| 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:   1. draft contracts between all the parties involved, if applicable; 2. terms and conditions of the provision of the account information services; 3. 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 EEA 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 the ZDG, 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 liability insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366 where the applicant intends to provide only account information services |  |  |  |  |  |  |
| *Business plan* | **The business plan to be provided by the applicant must contain:** | | |  |  |  |  |  |  |
| 4.1. | a | a marketing plan consisting of:   1. an analysis of the company's competitive position; 2. a description of account information service users, 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:   1. an income statement/forecast profit and loss 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; 2. explanations of the main lines of income and expenses, the financial debts and the capital assets; 3. a diagram and detailed breakdown of the estimated cash flows for the next three years |  |  |  |  |  |  |
| *Structural organisation* | **If the applicant is a natural person, the description of the structural organisation of the applicant's undertaking must contain the following information:** | | |  |  |  |  |  |  |
| 5.1 | a | an overall forecast of the staff numbers for the next three years |  |  |  |  |  |  |
|  | b | a description of the relevant operational outsourcing arrangements consisting of:   1. the identity and geographical location of the outsourcing provider; 2. the identities of the persons within the account information service provider that are responsible for each of the outsourced activities; 3. a detailed description of the outsourced activities and their main characteristics |  |  |  |  |  |  |
|  | c | a copy of draft outsourcing agreements |  |  |  |  |  |  |
|  | d | if applicable, a description of the use of branches and agents, including:   1. a mapping of the off-site and on-site checks that the applicant intends to perform of branches and agents; 2. the IT systems, processes and infrastructure that are used by the applicant's agents to perform activities on behalf of the applicant; 3. 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, indicating their identity and the nature of those links |  |  |  |  |  |  |
| **If the applicant is a legal person, the description of the structural organisation must contain the following information:** | | |  |  |  |  |  |  |
| 5.2. | 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:   1. the identity and geographical location of the outsourcing provider; 2. the identities of the persons within the payment institution that are responsible for each of the outsourced activities; 3. a detailed description of the outsourced activities and their main characteristics |  |  |  |  |  |  |
| d | a copy of draft outsourcing agreements |  |  |  |  |  |  |
| e | if applicable, a description of the use of branches and agents, including:   1. a mapping of the off-site and on-site checks that the applicant intends to perform of branches and agents; 2. the IT systems, processes and infrastructures that are used by the applicant's agents to perform activities on behalf of the applicant; 3. 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 |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Governance arrangements and internal control mechanisms* | **The applicant must provide a description of the governance arrangement and internal control mechanisms consisting of:** | | |  |  |  |  |  |  |
| 6.1 | 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 board of directors 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 an EU Member State, a description of the group governance |  |  |  |  |  |  |
| *Procedure for monitoring, handling and following up on security incidents and security-related customer complaints* | **The applicant must 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 must contain:** | | |  |  |  |  |  |  |
| 7.1 | 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 communication of these reports to internal or external bodies, notification of major incidents to national competent authorities under Article 102 ZDG 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 |  |  |  |  |  |  |
| *Process in place to file, monitor, track and restrict access to sensitive payment data* | **The applicant must provide a description of the process in place to file, monitor, track, and restrict access to sensitive payment data consisting of:** | | |  |  |  |  |  |  |
| 8.1 | a | a description of the flow of data classified as sensitive payment data in the context of the account information service provider'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 |  |  |  |  |  |  |
| *Business continuity arrangements* | **The applicant must provide a description of the business continuity arrangements consisting of the following information:** | | |  |  |  |  |  |  |
| 9.1 | 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 |  |  |  |  |  |  |
| *Security policy document* | 10.1 | 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:   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, the payment engine, the risk and fraud management engine, and customer accounting; 3. 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; 4. information on whether or not 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 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; 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:   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. 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:   1. the customer authentication procedure used for both consultative and transactional access; 2. 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; 3. 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 |  |  |  |  |  |  |
| *Identity and suitability assessment of directors and persons responsible for the management of the account information service provider* | 11.1 |  | See [FMA Communication 2013/07 – Guarantee in respect of the proper conduct of business](https://www.fma-li.li/files/list/fma-mitteilung-2013-07-englisch.pdf) |  |  |  |  |  |  |
|  | **As evidence of a professional liability insurance or comparable guarantee, the applicant for the provision of payment initiation services or account information services must provide the following information:** | | |  |  |  |  |  |  |
| *Professional indemnity insurance or a comparable guarantee for payment initiation services and account information services* | 12.1 |  | an insurance contract or other equivalent document confirming the existence of professional liability insurance or a comparable guarantee, with a cover amount that is compliant with EBA/GL/2017/08, showing the coverage of the relevant liabilities, and documentation of how the applicant has calculated the minimum amount, including all applicable components of the formula specified therein |  |  |  |  |  |  |

**Please note:**

If no explanation can be provided for one or more of the enumerated points, a written justification must be submitted to the FMA.

If the formation of an account information service provider 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) as well as in line with Liechtenstein data protection law.

Information regarding the processing of personal data, as well as details about the processing purpose, 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.html>.

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

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

| **For FMA use only** | |
| --- | --- |
| **Step** | **Date/comment** |
| Receipt of preliminary application |  |
| Demand for further documents |  |
| Receipt of definitive application |  |
| P1:  Result:  eligible for registration  not eligible for registration |  |
| P2:  Result:  eligible for registration  not eligible for registration |  |
| Decision and delivery of decision |  |
| CRM |  |
| Website/register/official journal |  |
| Internal information |  |

1. In addition to the address, please also provide, if known, the contact person with contact details (telephone number, e-mail address). [↑](#footnote-ref-1)