Onboarding Questionnaire

Aim of the questionnaire and how to complete it

The questionnaire contains the questions necessary for the processing of client access requests pursuant to Article 37 of Regulation (EU) No. 2017/392 and for monitoring the continued compliance of clients, which must be completed by any client wishing to join KELER prior to joining and at the frequency defined by KELER.

The questions are aimed at identifying legal / compliance, financial and operational risks.

KELER evaluates the answers to the questions on a risk basis, so it considers the legal/compliance, financial and operational risk factors in such a way that compliance with them supports the security, integrity and reputation of KELER and KELER's clients. Your organization becoming a client and your continued operation as a client shall not result in any way in KELER’s violating any law or KELER’s internal regulatory documents, whether in tax, money laundering or legal terms. Should any of these arise, KELER shall have the right to request any further information, documentation, on-site inspection, order test cases and to establish conditions that will prevent KELER from being subject to any breach of the law and its internal regulatory documents.

Please write the answers to our questions in the light blue boxes and, in case of re-filling, make your changes appear in the original document with the track changes function.

Thank you for your co-operation!

I. Compliance with legal criteria

Do you have a financial supervisory licence? If so, please list the authorised activities and indicate the supervisory authority.

☐ Yes.

Activities:

Name of supervisor authority, registered office, website:

☐ No.

Are you subject to money laundering prevention regulations in Hungary or a European Union Member State or equivalent? (Please attach Wolfsberg Questionnaire completed in the given year.)

☐ Yes.

Indicate the regulation:

☐ No.

Do you have an internal regulatory environment to prevent abuse or fraud?

☐ Yes.

☐ No.

Sanctions

Does your organisation have a registered office/branch/establishment, investment, activity or plans to have an activity in a country or geographical area subject to sanctions issued by the European Union, the United Nations or OFAC, or does it conduct business in such geographical areas?	☐ Yes. ☐ No.
Does your organization have any business relationship with a natural or legal person resident in a country subject to sanctions imposed by the European Union, the United Nations or OFAC, or owned or controlled by a sanctioned person, including intermediaries acting or engaged in transactions in the name or on behalf of sanctioned persons?	☐ Yes. ☐ No.

How does your organization ensure the proper use of accounts as required by the KELER General Business Rules and limited to securities settlements? Please briefly describe your procedure (e.g.: automated monitoring, manual controls or other measures)!

Significant supervisory or regulatory fines for actual or suspected violations or breaches of rules or regulations in the last five years (It is considered significant if the value of the fine exceeds EUR 80,000 (or the equivalent in other currencies) or if it is relevant in terms of onboarding.)

☐ Yes. Name of authority: Resolution date: Resolution summary: Remedial) measures taken: ☐ No.

Do you have a compliance officer responsible for the implementation of the compliance assurance programme?

☐ Yes. Name of the person holding this function: Position: Email address: Phone number: ☐ No.

II. Compliance with financial criteria

Please attach the audited financial statements for the previous financial year or provide the public access details of the financial statements.

Is your organization certified by an international credit rating agency(ies)?

If so, please provide the most recent published credit rating for your organization and the name of the credit rating agency.

If your organization does not have a public credit rating, please name your parent company and provide its most recent public credit rating(s) and the name of the credit rating agency.

☐Yes. Own credit rating: Name of credit rating agency: ☐No. Name of parent company: Credit rating of parent company: Name of credit rating agency:

III. Compliance with operational criteria

III.1. Questions on risk management

Does your organization perform stress tests on a regular basis?

	Is the risk relevant?	Do you perform stress tests?
Stress test for operational risks	☐ Yes ☐ No	☐ Yes ☐ No
Stress test for market risks	☐ Yes ☐ No	☐ Yes ☐ No
Stress test for credit and counterparty risks	☐ Yes ☐ No	☐ Yes ☐ No

Please confirm that your stress testing methodology is documented in your internal policies, which are regularly reviewed and reported to the management:

The stress test methodology has been laid down in internal rules.	☐ Confirmed ☐ Not confirmed If not, please specify:
The document describing the stress tests is being reviewed::	☐ six-monthly ☐ annually ☐ biannually ☐ other; please specify:
The results of stress tests that reveal the risks are reported to:	☐ the Board of Directors ☐ the management/executive board ☐ to other governing bodies ☐ not reported

Please provide information on whether the following applied to your organization in the past 36 months:

- litigation jeopardizing the organization's operation (even pending),

- your organization is subject to a penalty, measure or decision by the authorities.

Confirm that your organization has and applies risk management policies that ensure that credit, market, liquidity and concentration risks arising from business activities between your clients and the organizations) that provide you with liquidity (i.e. the parent company) are properly managed. Please confirm that relevant processes are documented in internal policies and that compliance is regularly monitored and reviewed.

The organization has risk management principles to manage credit, market, liquidity and concentration risks arising from the business activities.	☐ Confirmed ☐ Not confirmed
The policy containing the risk management principles is regularly reviewed:	☐ six-monthly ☐ annually ☐ biannually ☐ other, please specify:

Please specify whether, for the last two financial years, your organization has encountered any fault interrupting or halting operation that has led to a significant reduction or total loss of service quality (for example: permanent disruption of Internet-based service, inability to deliver services, inaccessible service, cases that disturb your daily processes, etc ...). In the details, indicate these problematic events, their duration, the number of errors, and their loss.

Please explain any incidents that have significantly reduced the quality of service for more than 3 months and the steps your organization has taken to address them.

Please confirm that your organization has internal processes in place to measure and manage operational risks across all areas of your organization:

The organization has:

A person with operational risk management responsibilities (e.g.: Operational Risk Manager)	☐ Yes ☐ No
Contact persons responsible for operational risk	☐ Yes ☐ No
Committee managing operational risk (i.e.: Operational Risk Management Committee)	☐ Yes ☐ No

Please confirm that the rules for the identification, measurement, management and reporting of operational risks, the rules for the collection of operational risk and other indicators and the procedures for the collection of operational risk events are set out in internal regulatory frameworks which are regularly reviewed.

The organization has a risk management framework and principles for managing operational risks.	☐ Confirmed ☐ Not confirmed
The date of the revision of the policy containing the Operational Risk Management principles is repeated on a regular basis:	☐ six-monthly ☐ annually ☐ biannually ☐ other, please specify:

III.2. Business Continuity (BCP), Disaster Recovery (DRP), Security Management and Technology System Protection

The information security questions (below) of the questionnaire do not need to be answered if KELER is provided with an information security certificate of your organization. Please present the following:

- certification report / certificate,
- name of the certifier
- scope of certification
- name of the standard applied.

If you either do not have certification or you do present it to KELER or the scope of the certification is not KELER relevant (see relevant access criteria), please answer the questions below.

KELER reserves the right to request answers to the questions below despite certification.

Business Continuity Capabilities (BCP)

Interpreted for KELER related processes

Please confirm that you have the following documentation for business continuity purposes *(Multiple answers are possible)*	☐ BCP Strategy and Regulations ☐ BCP plans updated within one year per process ☐ Testing minutes for BCP Plans ☐ Records of BCP events
Confirm that your business continuity policy and strategy addresses the following *(Multiple answers are possible)*	☐ Responsible persons and their duties ☐ Classification criteria of crisis ☐ Preparing for a crisis situation ☐ Response to a crisis situation ☐ Communication tasks ☐ Reporting obligation ☐ Business Continuity training ☐ Business Continuity Testing
Confirm that your business continuity plans are regularly tested *(Only one answer is possible)*	☐ We test them at least annually ☐ We test them, but less frequently than annually ☐ Not tested
Confirm that improvements have been made to test plans due to deficiencies discovered during business continuity testing *(Only one answer is possible)*	☐ Confirmed ☐ No such measures were required ☐ Not confirmed

Please specify when the last BCP test took place	(year)
Confirm that you have a alternative office site *(Only one answer is possible)*	☐ Confirmed ☐ Not confirmed
Confirm that your business continuity critical workforce has access to all necessary systems *(Only one answer is possible)*	☐ Confirmed ☐ Not confirmed

Disaster Recovery Capabilities (DRP)

Interpreted for KELER related processes

Please confirm that you have the following documentation for disaster recovery purposes *(Multiple answers are possible)*	☐ DRP Strategy and Regulations ☐ DRP plans updated per process / system within one year ☐ Testing minutes for DRP plans ☐ Records of DRP events
Confirm that the disaster recovery policies and strategies address the following *(Multiple answers are possible)*	☐ Responsible persons and their duties ☐ Preparing for disaster recovery situation ☐ Post-disaster recovery tasks ☐ Disaster recovery training ☐ Disaster Recovery Testing ☐ Contact details of external service providers
Confirm that your disaster recovery plans are regularly tested *(Only one answer is possible)*	☐ We test them at least annually ☐ We test them, but less frequently than annually ☐ Not tested
Confirm that improvements have been made in test plans due to deficiencies discovered during disaster recovery testing *(Only one answer is possible)*	☐ Confirmed ☐ No such measures were required ☐ Not confirmed
Please specify when the last DRP test was performed	(year)
Confirm that their disaster recovery critical workforce has access to all necessary systems *(Only one answer is possible)*	☐ Confirmed ☐ Not confirmed

Confirm that your organization has an RTO (Recovery Time Objective) value for CSD relevant processes *(Only one answer is possible)*	☐ Less than 2 hours ☐ Between 2 and 8 hours ☐ More than 8 hours

Security management system

Confirm that you have an information security organization that is independent of other departments. *(Only one answer is possible)*	☐ Confirmed ☐ Not confirmed
Does your organization have a quality assurance certification for information security (e.g.: ISO27001)? *(Only one answer is possible)*	☐ Yes. If yes, please specify the type, scope and date of certification: ☐ No
Does your organization have a management-approved information/cybersecurity strategy that covers future threats and planned improvements? *(Only one answer is possible)*	☐ Yes. If so, please provide the date of your last review: ☐ No
Does your organization have a management-approved information security/cybersecurity policy that includes management's commitment to meeting its security objectives? *(Only one answer is possible)*	☐ Yes. If yes, please provide the date of entry into force of the current version: ☐ No
Please confirm that your organization has the following documents: *(Multiple answers are possible)*	☐ Business impact and risk analysis based on international methodology ☐ Business impact analysis updated within one year ☐ Information security risk analysis updated within one year ☐ Action plan or risk list accepted by management
Does your organization have an information security policy that sets out the duties and responsibilities of users, IT, security, technology controls applied? *(Only one answer is possible)*	☐ Yes. If yes, please provide the date of entry into force of the current version: ☐ No

Please indicate which of your users have security awareness training for your organization. *(Multiple answers are possible)*	☐ Security training for new joiners ☐ Annual mandatory security awareness training ☐ Annual mandatory security awareness test ☐ Regular Safety Awareness Newsletter or Tests
Does your organization have a list of security requirements for system development? *(Only one answer is possible)*	☐ Confirmed ☐ Not confirmed
Frequency of reviewing information security / cybersecurity policies and regulations within the organization *(Only one answer is possible)*	☐ Annually ☐ Biannually ☐ If none, please provide frequency:
Confirm that your organization has an up-to-date list of critical service providers.	☐ Yes. If yes, please provide the date of your last review: ☐ No
If you join KELER as a CSD or market infrastructure, please list the critical service providers you have used.[1]	
Does your organization outsource information security functions or processes? *(Only one answer is possible)*	☐ Yes. If yes, please identify the security processes, party(ies) involved and specify its headquarter(s). ☐ No

[1] Pursuant to Article 69 (2) a) of Commission Delegated Regulation (EU) 2017/392.

Security technologies

What information security technical controls and processes do you have? *(Multiple answers are possible)*	Network security ☐ Firewall protection ☐ Web Application Firewall ☐ Intrusion Detection / Prevention System ☐ Network Access Control ☐ Network separation ☐ Web and mail filtering systems Endpoint protection ☐ Virus and malware protection ☐ Disk Encryption for End User Devices ☐ Mobile device protection Security Monitoring ☐ Central security event management system ☐ Periodic Vulnerability Test ☐ Incident management process ☐ Regular security training Physical security ☐ Video surveillance system ☐ Access Control System ☐ Physical intrusion protection system ☐ Manned security ☐ Building surveillance systems Data security ☐ Data leakage protection ☐ File encryption ☐ Database encryption ☐ Mail encryption Access management ☐ User and authorization management system ☐ Two-factor identification ☐ Technical user and password management solution

Supervision and audits

Confirm that over the past two years, the oversight authority has carried out a comprehensive information security audit at your organization *(Only one answer is possible)*	☐ Confirmed. Please provide the name and the seat of the authority! ☐ Not confirmed
Confirmation that over the past two years an independent audit firm has conducted a comprehensive information security audit of your organization *(Only one answer is possible)*	☐ Confirmed. Please enter your company name and registered office! ☐ Not confirmed
Please indicate the highest risk level of the observations made in the last two years.	
Confirm that you have a plan of action to remediate findings or management risk acceptation *(Only one answer is possible)*	☐ Confirmed ☐ Not confirmed
Have you experienced outside breaches of your system security rules in the last 12 months? *(Only one answer is possible)*	☐ Yes. If so, how do you reduce the risk of recurrence of similar events? ☐ No

III.3. Questions related to the organization's IT systems

Data centre redundancy

Confirm that you have a backup (secondary) data centre *(Only one answer is possible)*	☐ Confirmed. Please enter the distance between your data centres (in km): km ☐ Not confirmed

Backup policy and strategy

Please confirm that your organization has one of the structured back-up solutions. *(Multiple answers are possible)*	☐ Real time ☐ Mirrored with delay ☐ Daily ☐ Weekly ☐ Other

Capacity management

Confirm that your organization has capacity management. *(Only one answer is possible)*	☐ A capacity plan, supported with monitoring system and historical data, is prepared at least once a year ☐ There is only a monitoring system ☐ Not confirmed

III.4. Operation questions

Expected number of settlement orders (pcs/month)	
Expected transaction types	
Please indicate the currencies in which you plan to make settlement.	
Does your organization plan to communicate via KID or SWIFT?	☐ KID ☐ SWIFT
Do you plan to use a third party (proxy) to manage the account?	
Please describe to what extent the settlement and reconciliation processes are supported by your own systems and to what extent is automatic processing ensured.	

I hereby certify that the above provided facts and information are true and correct.

I declare that I will inform KELER immediately if there is any change in the information, circumstances or conditions presented in the questionnaire regarding the organization I represent.

Client / Organization name

Respondent's name, position, contact details (email/phone)

.....	.....
(Authorised signatory's name)	(Authorised signatory's name)
(Position)	(Position)
(Organization name)	(Organization name)

(Place): , (date (DD/MM/YYYY)):