KELER Depository Announcement – No. 9-01

On Access Management

Effective from: 22 January 2024

Table of Content

1. Introduction

The purpose of this Depository Announcement is that KELER Central Securities Depository Ltd. (hereinafter: 'KELER') makes publicity available the terms and conditions of access to certain services provided by it and the general procedure for evaluation of compliance with the access criteria pursuant to the provisions of Regulation (EU) No. 909/2014 (CSDR) of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU Regulation No. 236/2012 and Commission Delegated Regulation (EU) 2017/392 (RTS) supplementing Regulation (EU) No. 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorization, supervisory and operational requirements for central securities depositories.

KELER shall use the forms provided by Regulation (EU) No. 2017/394 (ITS) laying down implementing technical standards with regard to standard forms, templates and procedures for authorization, review and evaluation of central securities depositories, for the cooperation between authorities of the home Member State and the host Member State, for the consultation of authorities involved in the authorisation to provide banking-type ancillary services, for access involving central securities depositories, and with regard to the format of the records to be maintained by central securities depositories in accordance with Regulation (EU) No. 909/2014 of the European Parliament and of the Council to ensure that these rules are properly enforced.

The CSDR specifies, that CSDs established in the European Union shall provide access to participants according to the same principles, disclosed objective terms and non-discriminatory criteria, and lays down uniform procedural rules for the processing of requests for access and remedies for refusal.

This depository announcement (hereinafter: 'Depository Announcement') is approved by the Supervisory Authority, and it supplements the rules on participating in the Settlement system of KELER laid down in the General Business Rules of KELER (hereinafter: 'GBR'). The Depository Announcement sets out the rules governing the evaluation of requests, the rules for accepting and refusing access, the rules for regular and risk-based testing, and the rules for suspending and withdrawing access to each individual (Participants, CSDs, Other market infrastructures) having access to the Settlement system of KELER.

The terms used in the Depository Announcement shall have the same meaning as defined in the GBR.

Templates for submitting an application for access, refusing an application and lodging a complaint against a refusal with the content required by ITS are attached to the Depository Announcement.

2. General requirements for access

2.1. Access rules

KELER provides settlement services only to legal entities referred to in Section I.2.4 of the GBR.

The Depository Announcement contains the terms and conditions for access, refusal or withdrawal to the following services only:

- Services related to the access of the Settlement system for Participants (Article 33 of the CSDR),
- Services related to the access of the Settlement system for CSDs (Article 52 of the CSDR),
- Services related to the access of the Settlement system for Other market infrastructures, and provision of transaction feeds by the Central Counterparty and the trading venue to KELER (Article 53 of the CSDR).

These services may be used only after the Participant, the CSD and the Other market infrastructure (hereinafter: 'Joining Client') submits the information necessary to assess compliance with the access criteria as set out in the Depository Announcement, and once KELER has evaluated them, granted access and concluded the relevant contracts with the Joining Client. The Joining Client may submit their request for access in Hungarian or in English.

KELER concludes the contracts for the use of the service only if the Joining Client is granted access.

The Joining Client shall immediately notify KELER of any change in the Documentation during joining or after joining, or any change in compliance with the access criteria which results in it no longer meeting the access criteria.

If the Joining Client provides notification of the change, KELER shall examine the change no later than within 30 days of receiving the change notification and, if necessary, depending on the change, shall order the Joining Client to provide further declarations or documents, submit data, perform tests or authorise an on-site inspection.

If the Joining Client does not provide notification of the change within the given deadline, KELER may suspend or terminate the Joining Client's participation in the Settlement system.

If a change notified by the Joining Client or detected by KELER results in a change in the Documentation submitted by the Joining Client or in the compliance with the access criteria that would justify refusal of access, KELER may suspend or withdraw access, provided that the conditions prevail.

2.2. Access criteria

KELER sets the following access criteria.

A) Criteria in relation to the assessment of legal risks that are evaluated in the comprehensive risk analysis:

The Joining Client must

- provide complete and duly authenticated documents and declarations as defined in the GBR as conditions for opening an account (failure to meet this criterion excludes joining);
- meet the client category eligible for access by KELER (see Section I.2.4 of the GBR), (failure to meet this criterion excludes joining);
- ensure that KELER is able to implement the client identification and client due diligence measures set out in Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing and that the joining client complies with the obligations set out in the said legislation (failure to meet this criterion excludes joining);
- not have its registered office in a high-risk third country with strategic deficiencies, and its beneficial owner must not be resident in such countries (failure to meet this criterion excludes joining);
- not be an organization subject to financial and property restraint measures imposed by the European Union, or to sanctions lists of the United Nations Security Council or, on the basis of an individual risk assessment, to the sanctions lists of the U.S. Department of the Treasury, The Office of Foreign Assets Control (OFAC), or an organization whose beneficial owner or representative is subject to such measures (failure to meet this criterion excludes joining);
- not be an anonymous account-holding financial institution (failure to meet this criterion excludes joining);
- not be a fictitious bank or a financial institution having business correspondence with a fictitious bank (failure to meet this criterion excludes joining);
- apply Hungarian or equivalent regulations for the prevention of money laundering, and accordingly, they must perform the verification check of the identity of clients with access to accounts managed by KELER, and must also monitor access to these accounts;
- ensure that its internal procedures are suitable for ensuring that the account managed by KELER are used properly;
- refrain from any activity deemed as violation of any national and international sanctions (restricting measures), and must also have in place procedures for the prevention, discovery and reporting of violations of sanctions.

B) Criteria in relation to the assessment of financial risks that are evaluated in the comprehensive risk analysis:

The Joining Client must

- have sufficient resources, both for its current and future operations, to meet and maintain its financial obligations as required by its contract with KELER and its regulatory documents.

C) Criteria in relation to the assessment of operational risks that are evaluated in the comprehensive risk analysis:

The Joining Client must

- have an approved and documented Business Continuity Management system in place,
- have a documented and tested BCP plan in place for relevant procedures,
- have a documented and tested DRP plan in place for relevant procedures,
- have a cybersecurity system and regulation in place, prepared in view of internationally accepted standards,
- have in place cyber and IT security controls and implemented protection technology which is compliant with best industrial standards,
- have undergone independent audits performed by a state supervisory authority or internationally accepted auditor firm at least every two years, covering suitability of IT security,
- have its risk management framework proportionate with the risk profile, capital strength and business strategy of the company,
- ensure that its business operations do not pose an extraordinary risk to KELER and the settlement system operated by KELER, and its participants,
- have redundant data centers,
- have backup policy and strategy in place,
- have capacity management,
- have in place an appropriate infrastructure in view of its operations and activities,
- have control mechanisms embedded in procedures, and these controls must regularly be checked, and transformed as its operational model changes.

2.3. Main rules for assessing access

In this Depository Announcement KELER informs the Joining Client of the access criteria and provides or makes the request for access available on its website (hereinafter: 'Request for Access'). The initiation of the use of the service requires the submission of the request (Request for Access) provided in Annex 1 of the Depository Announcement.

The Joining Client shall submit the written Request for Access electronically (email address: clientservice@keler.hu), or by post. KELER is entitled to request the Joining Client to sign the Request for Access.

A Request for Access is considered suitable for assessment if it is duly completed by the Joining Client.

If the Request for Access is made by a legal entity who is obviously not entitled to use the services of KELER, KELER will refuse access, of which it shall notify the legal entity concerned by sending the template set out in Annex 3 to the Depository Announcement.

KELER shall notify the person responsible for the Request for Access, as indicated in the Request for Access, in writing, within a maximum of 3 business days, of the acceptance of the Request for Access or of any deficiencies in the Request for Access, via the email address indicated therein. If

the Request for Access has been submitted incompletely and is therefore not suitable for a substantive assessment, KELER shall inform the Joining Client that the Request for Access will be accepted upon its complete submission.

Following the receipt of the Request for Access, KELER sends to the Joining Client the list of documents to be made available to KELER and completed pursuant to Chapter I.2.4. of the GBR, which includes the Onboarding Questionnaire provided in Annex 5 of the Depository Announcement for the Joining Client and the account opening documentation templates.

Upon receipt of the required documents, KELER immediately verifies the compliance of the Joining Client with the access criteria and the adequacy of the documentation. KELER decides whether to grant or refuse access based on a risk assessment. KELER shall notify the Joining Client of the refusal within the deadline specified in this Depository Announcement for the given Joining Client pursuant to Annex 3 of the Depository Announcement, stating the reasons for the refusal. Should the refusal be based on a justification by which KELER would violate its mandatory legal provisions (e.g.: relevant provisions for KELER to prevent and combat money laundering and terrorist financing), KELER notifies the Joining Client of the refusal of access without any detailed justification however, KELER will inform the Central Bank of Hungary (hereinafter: 'Supervising Authority') of the detailed justification.

2.4. Rules of remedy relating to refusal or withdrawal of access

In the event of refusal or withdrawal of access, the Joining Client may lodge a complaint to the Supervising Authority within 1 month of receiving the decision containing the refusal or withdrawal.

If, based on the complaint of the Joining Client, the Supervising Authority determines that KELER has unjustifiably refused or withdrew access from the Joining Client and instructs KELER to grant access to the Joining Client, KELER shall grant access within 3 months (or if Joining Client is a central securities depository and a customised relationship requires significant IT development, unless otherwise agreed, within 8 months).

3. Rules of access to the securities settlement system for Participants

3.1. Defining the scope of the Participants

Participant: the person defined in Section 2 (1) j) of the Finality of Settlement Act.

The Participants are entitled to access and participate in the securities settlement system operated by KELER. KELER applies fair, open, public, transparent, objective and non-discriminatory access rules.

3.2. Access criteria

When access is requested by a Participant, KELER shall consider the legal, financial and operational risks arising from such access in accordance with the legal, financial and operational access criteria set out in this Depository Announcement.

KELER may change the access criteria due to changes in the regulatory environment, changes in the operation of KELER and the operation of markets. KELER will always publish the changes.

The Participant is obliged to comply with the access criteria, as well as the documents and declarations submitted in support of compliance with the access criteria. KELER assesses the compliance at regular intervals and in the event of an emerging risk, on an ad hoc basis. KELER may request the Participant to send the documents and declarations supporting compliance for the purpose of the assessment, and shall be entitled to perform the assessment specified in the GBR.

3.3. Rules for accepting access

The Participant may submit the Request for Access using the form in Annex 1 of the Depository Announcement, either electronically (email address: clientservice@keler.hu) or by post.

After confirmation of the acceptance of the Request for Access by KELER, the Participant shall send the Onboarding Questionnaire provided in Annex 5 to this Depository Announcement, duly completed and signed by the Participant, as well as the documentation required for account opening. Upon the request of KELER, the Participant shall send the additional documents required by KELER for compliance.

KELER shall evaluate without delay the documents provided to KELER in support of the Participant's compliance with the access criteria, and shall provide a written response to the Participant no later than one month after the submission of complete Documents for evaluation, using the template provided in Annex 2 of the Depository Announcement.

3.4. Rules for refusing access

KELER shall refuse access to a Participant only with a decision based on a comprehensive risk assessment, with a written justification specified in the template set out in Annex 3 of this Depository Announcement.

KELER shall notify the Participant in writing of the refusal decision within one month after the receipt of the complete Documents suitable for evaluation.

3.5. Regular review of compliance with Access Criteria and the assessment performed upon the emergence of risks

The Participant is obliged to comply with the access criteria, as well as the documents and declarations submitted in support of compliance with the access criteria. KELER assesses the Participant's compliance periodically in order to ensure compliance. During the regular review KELER evaluates the compliance of the Participant based on the evaluation of the up-to-date documents, and during the compliance review KELER evaluates the risks assessed, the documents and the declarations during the access evaluation.

The Participant is required to submit up-to-date documents within 30 days for regular review. If the Participant fails to prove their compliance with the access requirements within the set deadline, KELER may suspend the Participant until such compliance is confirmed, or may withdraw access if certain conditions prevail.

In the event that any risk to the operation of the Settlement System arises, KELER shall request the Participant to restore compliance by setting a deadline and, upon expiry of the deadline, shall assess the Participant's compliance based on the evaluation of the up-to-date documents. During the compliance review KELER evaluates the risks assessed during the access evaluation, the documents and the declarations.

3.6. Rules for suspension of the Participant and withdrawal of their access

KELER may suspend the Participants in the Settlement System who, on the basis of KELER's assessment carried out on a regular basis and in the event of risks endangering the operation of the Settlement System, do not comply with the access requirements or the documents and declarations submitted in support of compliance with the access criteria.

Furthermore, KELER shall suspend Participants in the Settlement system that consistently and regularly fail to deliver on the intended settlement date, as provided for in Article 7 (9) of the CSDR and Chapter I.2.5. and II.4.9 of the GBR, subject to prior consultation with the Supervisory Authority.

In the event of suspension of the Participant's access, KELER shall also apply the rules specified in the GBR relating to the suspension of the right to dispose over the account.

KELER shall withdraw access to the Settlement System for Participants who are no longer eligible to use the services of KELER, or do not terminate the circumstance giving rise to the suspension during the period of suspension.

The decision to suspend or withdraw access may be based on the same reasons as refuse of access, which KELER shall immediately notify the Participant. The Participant may lodge a complaint against the suspension decision to the Supervising Authority in accordance with the procedure

governing the refusal of the request for Access, and the Participant may only be exited if no complaint has been submitted or KELER has not been obliged to grant access by the Supervising Authority in the event of a complaint.

KELER shall lift the suspension of the Participant only after the Participant has reaffirmed that they are entitled to use the services of KELER and that, pursuant to the comprehensive risk assessment, they comply with the criteria, or if the Supervising Authority obligated KELER to grant (restore) access.

In the event of withdrawal of the Participant's access, KELER shall also apply the rules on termination of the account in the GBR.

4. Rules of access for Central Securities Depositories

4.1. Definition of the scope of CSDs

Central Securities Depository means a legal person that operates a securities settlement system provides at least one other core service listed in Section A of the Annex of CSDR.

The CSD shall be entitled to become a participant in another CSD (including also KELER) and to establish a standard (Article 50 of the CSDR) or customized (Article 51 of the CSDR) links with KELER upon prior notification.

According to Article 48 (2) CSDR, when establishing CSD links, KELER and the CSD requesting access must either submit a request for authorization to the competent authority as set out in Article 19 (1) e) CSDR or inform the competent and relevant authorities as set out in Article 19 (5) CSDR.

The rules set out in this Depository Announcement shall apply to the accession of a CSD. KELER shall conclude a separate agreement on cooperation with the CSD. Unless otherwise agreed by the two parties, KELER may charge the CSD a reasonable commercial fee for providing the customised link, in addition to its costs.

4.2. Access criteria

When access is requested by a CSD, KELER shall apply the rules set out for Participants in relation to the Access Criteria.

4.3. Rules for accepting access

Acceptance of access shall be subject to the rules for Participant access, with the proviso that after having evaluated without delay the documents provided by the CSD in support of its compliance with the Access Criteria, it shall provide a written response no later than 3 months after the provision of complete documentation suitable for evaluation by sending the template document as provided in Annex 2 to the Depository Announcement.

4.4. Rules for refusing access

KELER shall refuse access to the CSD only with a decision based on a comprehensive risk assessment, with a written justification specified in the template set out in Annex 3 of the Depository Announcement.

KELER shall notify the CSD in writing of the refusal decision within 3 months after the receipt of the complete Documents suitable for evaluation.

If the CSD requests KELER to establish a unique relationship, KELER may refuse the application solely on the basis of risk considerations (loss of market share cannot be used as a basis for refusing the application).

KELER shall refuse access only if such accession would endanger the smooth and orderly functioning of the financial markets or cause systemic risk, such refusal shall be based on a comprehensive risk assessment.

4.5. Regular review of compliance with Access Criteria and the assessment performed upon the emergence of risks

The CSD is obliged to comply with the Access Criteria, as well as the documents and declarations submitted in support of compliance with the Access Criteria. KELER assesses the CSD's compliance periodically in order to ensure compliance. During the regular review KELER evaluates the compliance of the CSD based on the evaluation of the up-to-date documents, and during the compliance review KELER evaluates the risks assessed, the documents and the declarations during the access evaluation.

The CSD is required to submit up-to-date documents within 30 days for regular review. If the CDS fails to prove their compliance with the access requirements within the set deadline, KELER may suspend the CSD until such compliance is confirmed, or may withdraw access if certain conditions prevail.

In the event that any risk to the smooth and orderly functioning of the financial markets or a systemic risk arises, KELER shall request the CSD to restore compliance by setting a deadline and, upon expiry of the deadline, shall assess the CSD's compliance based on the evaluation of the up-to-date documents. During the compliance review KELER evaluates the risks assessed during the access evaluation.

4.6. Rules for suspension of the CSD and withdrawal of their access

KELER may suspend the CSDs in the Settlement System who, on the basis of KELER's assessment carried out on a regular basis and in the event of risks endangering the smooth and orderly functioning of the financial markets, or a systemic risk, do not comply with the access requirements or the documents and declarations submitted in support of compliance with the Access criteria.

In the event of suspension of the CSD's access, KELER shall also apply the rules on the suspension of the right of disposal over the account specified in the GBR.

KELER shall withdraw access to the Settlement System for CSDs who are no longer eligible to use the services of KELER, or do not terminate the circumstance giving rise to the suspension during the period of suspension.

The decision to suspend or withdraw access may be based on the same reasons as refuse of access, of which KELER shall immediately notify the CSD. The CSD may lodge a complaint against the suspension decision to the Supervising Authority in accordance with the procedure governing the refusal of the request for Access, and the CSD may only be exited if no complaint has been submitted or KELER has not been obliged to grant access by the Supervising Authority in the event of a complaint.

KELER shall lift the suspension of the CSD only after they have reaffirmed that they are entitled to use the services of KELER and that they comply with the access criteria, or if the Supervising Authority obligated KELER to grant (restore) access.

In the event of withdrawal of the CSD's access, KELER shall also apply the rules specified in the GBR for the termination of the account.

5. Rules of access for other market infrastructures (central counterparties and trading venues)

5.1. Defining the scope of other market infrastructures

Other market infrastructure: Central Counterparty (a legal entity that substitutes clients for contracts in one or more financial markets, acting as buyer to all sellers and as sellers to all buyers) and Trading Venue (any regulated market, multilateral trading facility (MTF) or organised trading system).

KELER shall provide a Central Counterparty or a Trading Venue with access to its securities settlement system in a non-discriminatory and transparent manner.

Pursuant to Section 53 (1) of the CSDR, the Central Counterparty and the Trading Venue shall provide transaction feeds to KELER on request in a non-discriminatory and transparent manner. KELER shall conclude a separate agreement on the use of the transaction feeds provided by the Other Market Infrastructure.

5.2. Access criteria

When access is requested by the Other Market Infrastructure, KELER shall consider the legal, financial and operational risks arising from such access in accordance with the legal, financial and operational access criteria set out in this Depository Announcement.

KELER may change the access criteria due to changes in the regulatory environment, changes in the operation of KELER and the operation of markets. KELER will always publish the changes.

During the joining of Other Market Infrastructure that only provides transaction feeds to KELER, KELER assesses whether it needs to make any significant changes to its operations that would affect its risk management procedures and jeopardise the smooth functioning of the KELER Settlement System, including the implementation of continuous manual processing.

The Other market infrastructure is obliged to comply with the access criteria, as well as the documents and declarations submitted in support of compliance with the access criteria. KELER assesses the compliance at regular intervals and in the event of an emerging risk. KELER may request the Other market infrastructure to send the documents and declarations supporting the compliance for the purpose of the assessment, and shall be entitled to perform the assessment specified in this GBR.

5.3. Rules for accepting access

Acceptance of access shall be subject to the rules for Participant access, with the proviso that after having evaluated without delay the documents provided by the Other Market Infrastructure in support of its compliance with the Access Criteria, it shall provide a written response no later than

3 months after the provision of complete documentation suitable for evaluation by sending the template document as provided in Annex 2 to the Depository Announcement.

5.4. Rules for refusing access

KELER shall refuse access to the Other market infrastructure only with a decision based on a comprehensive risk assessment, with a written justification specified in the template set out in Annex 3 of this Depository Announcement.

KELER shall notify the Other market infrastructure in writing of the refusal decision within three month after the receipt of the complete Documents suitable for evaluation.

If the Other market infrastructure submits a request for access to KELER, KELER may refuse access solely on the basis of risk considerations (loss of market share cannot be used as a basis for refusing the application).

KELER shall deny access only where such access would affect the smooth and orderly functioning of the financial markets or cause systemic risk.

5.5. Regular review of compliance with Access Criteria and the assessment performed upon the emergence of risks

The Other market infrastructure is obliged to comply with the access criteria, as well as the documents and declarations submitted in support of compliance with the access criteria. KELER assesses the Other Market Infrastructure's compliance periodically in order to ensure compliance. During the regular review KELER evaluates the compliance of the Other Market Infrastructure based on the evaluation of the up-to-date documents, and during the compliance review KELER evaluates the risks assessed, the documents and the declarations during the access evaluation.

The Other Market Infrastructure is required to submit up-to-date documents within 30 days for regular review. If the Other Market Infrastructure fails to prove their compliance within the set deadline, KELER may suspend the access of the Other Market Infrastructure until such compliance is confirmed, or may withdraw access if certain conditions prevail.

In the event of the emergence of systemic risks that threaten the smooth and orderly functioning of the financial markets or, in the case of Other Market Infrastructure that provides only transaction feeds to KELER, if there are significant changes affecting KELER's operations, that affect the risk management procedures of KELER and jeopardises the smooth operation of KELER's Settlement System, including the execution of continuous manual processing, KELER calls on the Other Market Infrastructure to restore compliance by setting a deadline, after which it shall assess the Other Market Infrastructure's compliance based on an evaluation of the up-to-date documents. During the compliance review KELER evaluates the risks assessed during the access evaluation.

5.6. Rules for suspension of the Other market infrastructure and withdrawal of their access

KELER may suspend Other Market Infrastructure in the Settlement System who, on the basis of KELER's assessment carried out on a regular basis and in the event of risks endangering the smooth and orderly functioning of the financial markets, or a systemic risk, does not comply with the access requirements or the documents and declarations submitted in support of compliance with the Access criteria.

In the event of suspension of the Other market infrastructure's access, KELER shall also apply the rules on the suspension of the right to dispose over the account in the GBR.

KELER shall withdraw access to the Settlement System for Other market infrastructures who are no longer eligible to use the services of KELER, or do not terminate the circumstance giving rise to the suspension during the period of suspension.

The decision to suspend or withdraw access may be based on the same reasons as the refusal of access, of which KELER shall immediately notify the Other market infrastructure. The Other market infrastructure may lodge a complaint against the suspension decision to the Supervising Authority in accordance with the procedure governing the refusal of the request for Access, and the Other market infrastructure may only be exited if no complaint has been submitted or KELER has not been obliged to grant access by the Supervising Authority in the event of a complaint.

KELER shall lift the suspension of the Other market infrastructure only after the they have reaffirmed that they are entitled to use the services of KELER and that they comply with the access requirements, or if the Supervising Authority obligated KELER to grant (restore) access.

In the event of withdrawal of the Other market infrastructure's access, KELER shall also apply the rules on the termination of the account specified in the GBR.

Forms related to access

Annex 1 - Request for Access for Participants requesting the establishment of a link with the CSDs or for the request for access of Other Market Infrastructures

Annex 2 - Notice form for the positive response to the request for access of Participants, CSDs and Other Market Infrastructures

Annex 3 - Form to be applied in the case of refusal of the request for access of Participants, and for the refusal of access of CSDs and Other Market Infrastructures

Annex 4 - Complaint Form: form to be applied in the case of refusal of the request for access of Participants, and for the refusal of access of CSDs and Other Market Infrastructures

Annex 5 - Onboarding Questionnaire

Should you need any further general information about what is described above, we shall be happy to be at your disposal if you send us and email to clientservice@keler.hu.

Annex 1

Request for Access for Participants requesting the establishment of a link with the CSDs or for the request for access of Other Market Infrastructures

I. General information

Sender (requesting party):

Addressee (receiving party):

Date of request for access:

Reference number given by the requesting party:

II. Identification of the requesting party

Corporate name of requesting party:

Country of origin:

Legal address:

LEI code:

Name and contact details of the person responsible for the request:

Name:

Position:

Phone number:

Email address:

III. Services forming the object of the request

Types of services:

Description of services:

IV. Identification of authorities

Name and contact details of the competent authority of the requesting party:

Name:

Position:

Phone number:

Email address:

Name and contact details of the relevant authority referred to in Article 12 (1) a) of Regulation 909/2014/EU:

Name:

Position:

Phone number:

Email address:

V. Any other relevant information and/or documents

Please provide an estimate of the number and average transaction value of the settlement transactions expected on the securities account opened at KELER on an annual/monthly basis, as well as the expected size of the portfolio safekeeping in the account. (For Other Market Infrastructures only if it also wishes to open an account.)

Annex 2

Notice form for the positive response to the request for access of Participants, CSDs and Other Market Infrastructures

I. General information

Sender (receiving party):

Addressee (requesting party):

Date of request for access:

Reference number given by the requesting party:

Date of receipt of the request for access:

Reference number given by the receiving party:

II. Identification of the receiving CSD

Corporate name of receiving party:

Country of origin:

Legal address:

LEI code:

Name and contact details of the person responsible for the assessment of the request:

Name:

Position:

Phone number:

Email address:

III. Identification of the requesting party

Corporate name of requesting party:

Country of origin:

Legal address:

LEI code:

Name and contact details of the person responsible for the request:

Name:

Position:

Phone number:

Email address:

Access granted YES

IV. Identification of authorities

Name and contact details of the competent authority of the receiving party:

Name:

Position:

Phone number:

Email address:

Name and contact details of the relevant authority referred to in Article 12 (1) a) of Regulation 909/2014/EU:

Name:

Position:

Phone Number:

Email address:

V. Any other relevant information and/or documents

Annex 3

Form to be applied in the case of refusal of the request for access of Participants, and for the refusal of access of CSDs and Other Market Infrastructures

I. General information

Sender (receiving CSD):

Addressee (requesting party):

Date of request for access:

Reference number given by the requesting party:

Date of receipt of the request for access:

Reference number given by the receiving party:

II. Identification of the receiving CSD

Corporate name of the receiving CSD:

Country of origin:

Legal address:

LEI code:

Name and contact details of the person responsible for the assessment of the request for access:

Name:

Position:

Phone number:

Email address:

III. Identification of the requesting party

Corporate name of requesting party:

Country of origin:

Legal address:

LEI code:

Name and contact details of the person responsible for the request for access:

Name:

Position:

Phone number:

Email address:

IV. Risk analysis of the request for access

Legal risks resulting from the provision of services:

Financial risks resulting from the provision of services:

Operational risks resulting from the provision of services:

V. Outcome of the risk analysis

Access would affect the risk profile of the CSD	YES	NO
Access would affect the smooth and orderly functioning of the financial markets	YES	NO
Access would cause systemic risk	YES	NO

In case of refusal of access, a summary of the reasons for such a refusal:

Deadline for complaint by the requesting party to the competent authority of the receiving CSD:

Access granted NO

VI. Identification of authorities

Name and contact details of the competent authority of the receiving CSD:

Name:

Position:

Phone number:

Email address:

Name and contact details of the relevant authority referred to in Article 12 (1) a) of Regulation 909/2014/EU:

Name:

Position:

Phone number:

Email address:

VII. Any other relevant information and/or documents

Annex 4

Complaint Form: form to be applied in the case of refusal of the request for access of Participants, and for the refusal of access of CSDs and Other Market Infrastructures

I. General information

Sender (requesting party):

Addressee (competent authority of receiving CSD):

Date of request for access:

Reference number given by the requesting party:

Date of receipt of the request for access:

Reference number given by the receiving party:

II. Identification of the requesting party

Corporate name of requesting party:

Country of origin:

Legal address:

LEI code:

Name and contact details of the person responsible for the request:

Name:

Position:

Phone number:

Email address:

III. Identification of the receiving CSD

Corporate name of the receiving CSD:

Country of origin:

Legal address :

Name and contact details of the person responsible for the assessment of the request for access:

Name:

Position:

Phone number:

Email address:

IV. Comments of the requesting party in relation to the risk assessment of the request for access conducted by the receiving CSD and the reasons for refusal of access

Comments of the requesting party on the legal risks resulting from the provision of services:

Comments of the requesting party on the financial risks resulting from the provision of services:

Comments of the requesting party on the operational risks resulting from the provision of services:

Comments of the requesting party concerning the refusal to provide the services referred to in Section A 1 of the Annex to Regulation 909/2014/EU applicable to the specific issue of securities:
Comments of the requesting CSD on the reasons of the receiving party for refusal of access:

Any relevant additional information:

V. Annexes
Copy of the initial application for access submitted by the requesting party to the receiving CSD
Copy of the response of the receiving CSD to the initial request for access

VI. Any other relevant information and/or documents

Annex 5

Onboarding Questionnaire

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)): .....