

KELER Ltd. Depository Announcement -

No. 9-01

On Access Management

Effective from: 17 December 2020

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 authorisation, 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 authorisation, 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 with regard to settlement services, that CSDs established in the European Union shall provide access to those services 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 a Settlement laid down in the General Business Rules of KELER (hereinafter: 'ÁÜSZ'). 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) who uses the securities services (settlement services) specified herein.

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

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

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 (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. If the Joining Client does not have a LEI code, they must request a LEI code before (or at the latest simultaneously with it) submitting their access request. 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 Contract Documentation 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 shall apply the consequences specified in the ÁÜSZ for the client's failure to notify.

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

KELER provides services only to legal entities referred to in Section 2.1 of the ÁÜSZ. Accordingly, KELER shall not provide access to its services, especially to:

- legal entities for which KELER is unable to implement client identification and client due diligence measures specified in Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing;
- natural persons;
- clients with strategic deficiencies with registered office in a high-risk third country or clients whose beneficial owners are effectively resident in such countries;
- financial and property restraint measures ordered by the European Union or organisations subject to United Nations sanctions lists or organisations and organisations the beneficial owner or representative of which is subject to such measures;
- financial institutions managing anonymous accounts,
- fictitious banks or financial institutions that have business correspondence relation with fictitious banks.

2.2. Main rules for assessing access

In Section 2.1 of the ÁÜSZ 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, with Annexes 5 and 6 annexed thereto.

The Joining Client shall submit the written Request for Access electronically (e-mail address: clientservice@keler.hu), and - the original copy, duly signed - by post.

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

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

KELER shall notify the person responsible for the Request for Access indicated in the application of the receipt or incompleteness of the Request for Access in writing, using the e-mail address specified in the Request for Access. If KELER informs the Joining Client that the request for Access has been submitted incompletely and therefore the request for Access is not suitable for substantive assessment, the request for Access will be received when the submission is complete.

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 Section 2.1 of the ÁÜSZ (Access Documents), which includes the Onboarding Questionnaire provided in Annex 7 of the Depository Announcement for the Joining Client and the Contract Documentation templates.

Upon receipt of the Access Documents, KELER verifies the compliance of the Joining Client with the access criteria and the adequacy of the Contract 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 the 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.

2.3. 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



KELER Central Securities Depository Ltd.

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 participation criteria.

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 order to assess the legal, financial and operational risks arising from the access, KELER defines the legal, financial and operational access criteria in Section 2.1 of the ÁÜSZ.

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

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 the compliance for the purpose of the assessment, and shall be entitled to perform the assessment specified in Section 2.13 of this ÁÜSZ.

3.3. Rules for accepting access

The Participant may submit the Request for Access electronically (e-mail cím: clientservice@keler.hu) using Annex 1 of the Depository Announcement and the templates provided in Annexes 5 and 6 constituting the annexes thereof, and - the original copies, duly signed - by post.

After KELER confirms the receipt of the Request for Access, the Participant shall send the documents specified for compliance with the Access Criteria in Section 2.1 of the ÁÜSZ, i.e. the fully completed and duly signed copy of the Onboarding Questionnaire provided in Annex 7 of the Depository Announcement and the Contract Documentation. 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 Access Documents for evaluation, using the template provided in Annex 2 of the Depository Announcement.

3.4. Rules for refusal access

KELER shall refuse access to the 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 the Depository Announcement.

KELER shall notify the Participant in writing of the refusal decision within one month after the receipt of the complete Access 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 with the access criteria periodically in order to ensure compliance. During the regular review KELER evaluates the compliance of the Participant with the access criteria based on the evaluation of the up-to-date Access Documents, and during the compliance review KELER evaluates the risks assessed during the access evaluation.

The Participant is required to submit up-to-date Access Documents within 30 days for regular review. If the Participant fails to prove their compliance with the Access Criteria within the set time limit, 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 with the Access Criteria based on the evaluation of the up-to-date Access Documents. During the compliance review KELER evaluates the risks assessed during the access evaluation.

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 criteria specified in Section 2.1 of the ÁÜSZ or the documents and declarations submitted in support of the compliance with the access criteria.

In the event of suspension of the Participant's access, KELER shall also apply the rules on the suspension of the right to dispose over the account in the ÁÜSZ

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, i.e. they do not fulfil the access criteria set out in the ÁÜSZ.

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 they comply with the access 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 ÁÜSZ.

4. Rules of access for other CSDs

1.1. Definition of the scope of other 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 relationship with KELER upon prior notification.

3.2. Access criteria

When access is requested by a CSD, KELER shall consider the legal, financial and operational risks arising from such access. In order to assess the legal, financial and operational risks arising from the access, KELER defines the legal, financial and operational Access Criteria in Section 2.1 of the ÁÜSZ.

KELER may change the Access Criteria due to changes in the regulatory environment, changes in the operation of KELER and the operation of markets. In all cases, KELER will publish the changes in the ÁÜSZ.

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 compliance at regular intervals and in the event of an emerging risk. KELER may request the CSD 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 Section 2.13 of this ÁÜSZ.

3.3. Rules for accepting access

The CSD may submit the Request for Access electronically (e-mail cím: clientservice@keler.hu) using Annex 1 of the Depository Announcement and the templates provided in Annexes 5 and 6 constituting the annexes thereof, and - the original copies, duly signed - by post. After KELER confirms the receipt of the Request for Access, the CSD shall send the documents specified for compliance with the Access Criteria in Section 2.1 of the ÁÜSZ, i.e. the fully completed and duly signed copy of the Onboarding Questionnaire provided in Annex 7 of the Depository Announcement and the Contract Documentation.

KELER shall evaluate without delay the documents provided to KELER in support of the CSD's compliance with the access criteria, and shall provide a written response to the CSD no later than three months after the submission of complete Access Documents for evaluation, using the template provided in Annex 2 of the Depository Announcement. Upon the request of KELER, the CSD shall send the additional documents required by KELER for compliance.

3.4. Rules for refusal 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 three months after the receipt of the complete Access Documentation 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.

4.1. 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 with the access criteria periodically in order to ensure compliance. During the regular review KELER evaluates the compliance of the CSD with the access criteria based on the evaluation of the up-to-date Access Documents, and during the compliance review KELER evaluates the risks assessed during the access evaluation.

The CSD is required to submit up-to-date Access Documents within 30 days for regular review. If the CSD fails to prove their compliance with the Access Criteria within the set time limit, KELER may suspend the CSD until such compliance is confirmed, or may withdraw their 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 with the Access Criteria based on the evaluation of the up-to-date Access Documents. During the compliance review KELER evaluates the risks assessed during the access evaluation.

4.2. 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 criteria specified in Section 2.1 of the ÁÜSZ or the documents and declarations submitted in support of the 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 ÁÜSZ.

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, i.e. they do not fulfil the access criteria set out in the ÁÜSZ.

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 ÁÜSZ (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.

5.2. Access criteria

When access is requested by an Other market infrastructure, KELER shall consider the legal, financial and operational risks arising from such access. In order to assess the legal, financial and operational risks arising from the access, KELER defines the legal, financial and operational access criteria in Section 2.1 of the ÁÜSZ.

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

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 Section 2.13 of this ÁÜSZ.

5.3. Rules for accepting access

The Other market infrastructure may submit the Request for Access electronically (e-mail clientservice@keler.hu) using Annex 1 of the Depository Announcement and the templates provided in Annexes 5 and 6 constituting the annexes thereof, and - the original copies, duly signed - by post.

After KELER confirms the receipt of the Request for Access, the Other market infrastructure shall send the documents specified for compliance with the Access Criteria in Section 2.1 of the ÁÜSZ, i.e. the fully completed and duly signed copy of the Onboarding Questionnaire provided in Annex 7 of the Depository Announcement and the Contract Documentation. Upon the request of KELER, the Other market infrastructure shall send the additional documents required by KELER for compliance.

KELER shall evaluate without delay the documents provided to KELER in support of the Other market infrastructure's compliance with the access criteria, and shall provide a written response to the Other market infrastructure no later than three months after the

submission of complete Access Documents for evaluation, using the template provided in Annex 2 of the Depository Announcement.

5.4. Rules for refusal 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 the Depository Announcement.

KELER shall notify the Other market infrastructure in writing of the refusal decision within three month after the receipt of the complete Access 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 with the access criteria periodically in order to ensure compliance. During the regular review KELER evaluates the compliance of the Other market infrastructure with the access criteria based on the evaluation of the up-to-date Access Documents, and during the compliance review KELER evaluates the risks assessed during the access evaluation.

The Other market infrastructure is required to submit up-to-date Access Documents within 30 days for regular review. If the Other market infrastructure fails to prove their compliance with the Access Criteria within the set time limit, KELER may suspend the Other market infrastructure until such compliance is confirmed, or may withdraw their 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 Other market infrastructure to restore compliance by setting a deadline and, upon expiry of the deadline, shall assess the Other market infrastructure's compliance with the Access Criteria based on the evaluation of the up-to-date Access 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 the Other market infrastructures 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 criteria specified in Section 2.1 of the ÁÜSZ or the documents and declarations submitted in support of the 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 ÁÜSZ.

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, i.e. they do not fulfil the access criteria set out in the ÁÜSZ.

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

- Annex 1 -** Request for Access for Participants requesting the establishment of a relationship with the CSDs or for the requests for access between CSDs and Other market infrastructures
- Annex 2 -** Notice form for the positive response to the request for the establishment of a relationship between the Participants and the CSDs, or to the request for access between 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 -** Declaration of the legal status of the Participants, CSDs and Other market infrastructures requesting access to the CSD
- Annex 6 -** Declaration of the services that the Participants, CSDs and Other market infrastructures requesting access to the CSD intend to use
- Annex 7 -** 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 an e-mail to ugyfelszolgalat@keler.hu.

Budapest, 17 December 2020.

KELER Ltd.

Annex 1

Request for access for Participants requesting the establishment of a relationship with the CSDs or for the requests for access between CSDs and Other market infrastructures (Annexes 5 and 6 are also to be attached)

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

Official address

LEI

Name and contact details of the person responsible for the request (name, position, phone number, e-mail address)	Name	Position	Phone number	E-mail address
--	------	----------	-----------------	-------------------

III. Services that form 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	E-mail 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	E-mail 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.

Annex 2

Template for the positive response to the request for the establishment of a relationship between the Participants and the CSDs, or to the request for access between 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

Official address

LEI

Name and contact details of the person responsible for the assessment
Name Position Phone E-mail
of the request (name, function, phone number, e-mail address) number address

III. Identification of the requesting party

Corporate name of requesting party

Country of origin

Official address

LEI

Name and contact details of the person responsible for the request
Name Position Phone E-mail
(name, position, phone number, e-mail address) number address

Access granted YES

IV. Identification of authorities

Name and contact details of the competent authority of the receiving
Name Position Phone E-mail
party (primary contact person, name, function, phone number, e-mail number address
address)

Name and contact details of the relevant authority referred to in
Name Position Phone E-mail
Article 12(1) a) of Regulation 909/2014/EU (primary contact person, number address
name, function, phone number, e-mail address)



KELER Central Securities Depository Ltd.

V. Any other relevant information and/or documents

Annex 3

Template for the refusal of access to a CSD

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

Official address

LEI

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

Name Position Phone number

E-mail address

III. Identification of the requesting party

Corporate name of requesting party

Country of origin

Official address

LEI

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

Name Position Phone number

E-mail 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

YES

NO

financial markets

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	E-mail 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	E-mail address
--	------	----------	--------------	----------------

VII. Any other relevant information and/or documents

Annex 4

Template for the submission of a complaint in the event of the refusal of access to a CSD

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

Official address

LEI

Name and contact details of the person responsible for the request for access (name, function, phone number, e-mail address)

III. Identification of the receiving CSD

Corporate name of the receiving CSD

Country of origin

Official address

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

Name	Position	Phone number	E-mail 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

Declaration of the legal status of the Joining Client requesting access to the CSD

Please indicate in the table below which client category the organisation(s) represented by you falls into, in your opinion:

Client category	Response ¹
Credit institution	
Payment institution	
Electronic money issuing institution	
Investment enterprise	
Commodities exchange service provider	
Hungarian State Treasury	
Államadósság Kezelő Központ (Government Debt Management Agency)	
Magyar Nemzeti Bank (Central Bank of Hungary)	
The central bank of the European Union member state	
European Central Bank	
Central counterparty	
Central Securities Depository	
Other market infrastructure (Trading Venue, regulated market, multilateral trading facility or organized trading facility)	

If in accordance with the your opinion the organisation represented by you does not fall into any of the categories listed above, please provide the definition that you consider most appropriate below.

¹ Please indicate 'x' or '✓' to the selected client category

Annex 6

Declaration of services that the Joining Client requesting access to the CSD intends to use

Core activity	Scope of services	Scope of services intended to be used ²	A brief description of the service intended to be used ³
Central securities depository activity	Central securities depository activities		
	issuance of ISIN code		
	Central register of securities and account management		
	Services related to dematerialised securities		
General depository activity	Custody of physical securities		
	Depository services related to dematerialised securities issued in Hungary and physical securities kept in fungible custody at KELER		
	Physical invalidation and destroying of physical securities and coupons		
Cash and securities account management	Securities account management and related account operations		
	Cash account management and related account operations (deposit settlement account, custody account)		
International market services	Settlement services for foreign securities		
	Management of corporate events relating to foreign securities		
	Tax procedure relating to foreign securities		
Other services	Collateral valuation and collateral verification for third parties		

² Please indicate 'x' or '✓' next to the name of the service intended to be used

³ If the service intended to be used by You is different from those in the General Business Rules of KELER, please briefly state the need/expectation for the service.



KELER Central Securities Depository Ltd.

	Trade reporting to the trade repository		
	Transparency reports		
	Reporting of transactions to the competent authority		
	Transmission of data to the ACER		
	LEI code issue		
	Paying agent activity		
	Share Book keeping		
	Organisation of General Meeting		



Annex 7

Onboarding Questionnaire

KELER Central Securities Depository Ltd.



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 organisation becoming a client and your continued operation as a client shall not result in any way in KELER's violating any law, regulation, regulation or its own rules, 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, ordering test cases and to establish conditions that will prevent KELER from being subject to any breach of its law and regulations.

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

Sanctions

<p>Does your organisation have headquarter / branch / establishment which invests, operates or plans to operate in Cuba / Crimea / Iran / North Korea / Sudan / Syria or do business in these geographical areas?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>Does your organisation have any business relationship with any natural or legal person resident in Cuba / Iran / North Korea / Sudan / Syria or with any legal person owned or controlled, directly or indirectly by a natural or legal person resident in Cuba / Iran / North Korea / Sudan / Syria, including intermediaries acting or involved in the transaction on behalf of or in the name of Cuban / Crimean / Iranian / North Korean / Sudanese / Syrian legal entities ?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>

How does your organisation ensure that your account is used properly? Please briefly describe your procedure! (e.g.: automated monitoring, manual controls or other measures)

I. Compliance with financial criteria

Please confirm that your organisation has sufficient financial resources to meet its future contractual obligations to the CSD.

- confirmed
- not confirmed

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

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

If your organisation 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:

II. Compliance with operational criteria

III.1 Questions on risk management

Does your organisation perform stress tests on a regular basis?

	Is the risk relevant?	Do you perform stress tests?
Stress test for operational risks	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Stress test for market risks	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Stress test for credit and counterparty risks	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> 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	<input type="checkbox"/> confirmed <input type="checkbox"/> not confirmed If not, please specify:
The document describing the stress tests is being reviewed:	<input type="checkbox"/> six-monthly: <input type="checkbox"/> annually <input type="checkbox"/> biannually <input type="checkbox"/> other; please specify:
The results of stress tests that reveal the risks are reported to:	<input type="checkbox"/> the Board of Directors <input type="checkbox"/> the management/executive board <input type="checkbox"/> to other governing bodies <input type="checkbox"/> not reported.

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

- litigation jeopardizing the organisation’s operation (even pending),

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

Confirm that your organisation has and applies risk management policies that ensure that credit, market, liquidity and concentration risks arising from business activities between your clients and the organisation(s) 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.

<p>The organisation has risk management principles to manage credit, market, liquidity and concentration risks arising from the business activities.</p>	<p><input type="checkbox"/> confirmed <input type="checkbox"/> not confirmed</p>
<p>The policy containing the risk management principles is regularly reviewed:</p>	<p><input type="checkbox"/> six-monthly: <input type="checkbox"/> annually <input type="checkbox"/> biannually <input type="checkbox"/> other, please specify:</p>



KELER Central Securities Depository Ltd.

Please specify whether, for the last two financial years, your organisation 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 organisation has taken to address them.

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

The organization has:

A person with operational risk management responsibilities (e.g.: Operational Risk Manager)	<input type="checkbox"/> Yes <input type="checkbox"/> No
Contact persons responsible for operational risk	<input type="checkbox"/> Yes <input type="checkbox"/> No
Committee managing operational risk (i.e.: Operational Risk Management Committee)	<input type="checkbox"/> Yes <input type="checkbox"/> 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 organisation has a risk management framework and framework for managing operational risks.	<input type="checkbox"/> confirmed <input type="checkbox"/> not confirmed
The date of the revision of the policy containing the Operational Risk Management principles is repeated on a regular basis:	<input type="checkbox"/> six-monthly: <input type="checkbox"/> annually <input type="checkbox"/> 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 organisation. 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

<p>Please confirm that you have the following documentation for business continuity purposes <i>(Multiple answers are possible)</i></p>	<input type="checkbox"/> BCP Strategy and Regulations <input type="checkbox"/> BCP plans updated within one year per process <input type="checkbox"/> Testing minutes for BCP Plans <input type="checkbox"/> Records of BCP events
<p>Confirm that your business continuity policy and strategy addresses the following <i>(Multiple answers are possible)</i></p>	<input type="checkbox"/> Responsible persons and their duties <input type="checkbox"/> Classification criteria of crisis <input type="checkbox"/> Preparing for a crisis situation <input type="checkbox"/> Response to a crisis situation <input type="checkbox"/> Communication tasks <input type="checkbox"/> Reporting obligation <input type="checkbox"/> Business Continuity training <input type="checkbox"/> Business Continuity Testing
<p>Confirm that your business continuity plans are regularly tested <i>(Only one answer is possible)</i></p>	<input type="checkbox"/> We test them at least annually <input type="checkbox"/> We test them, but less frequently than annually <input type="checkbox"/> Not tested



KELER Central Securities Depository Ltd.

Confirm that improvements have been made to test plans due to deficiencies discovered during business continuity testing. <i>(Only one answer is possible)</i>	<input type="checkbox"/> Confirmed <input type="checkbox"/> No such measures were required <input type="checkbox"/> Not confirmed
Please specify when the last BCP test took place (year)
Confirm that you have a alternative office site <i>(Only one answer is possible)</i>	<input type="checkbox"/> Confirmed <input type="checkbox"/> Not confirmed
Confirm that your business continuity critical workforce has access to all necessary systems. <i>(Only one answer is possible)</i>	<input type="checkbox"/> Confirmed <input type="checkbox"/> Not confirmed

Disaster Recovery Capabilities (DRP)

Interpreted for KELER related processes

<p>Please confirm that you have the following documentation for disaster recovery purposes <i>(Multiple answers are possible)</i></p>	<p><input type="checkbox"/> () DRP Strategy and Regulations <input type="checkbox"/> () DRP plans updated per process / system within one year <input type="checkbox"/> () Testing minutes for DRP plans <input type="checkbox"/> () Records of DRP events</p>
<p>Confirm that the disaster recovery policies and strategies address the following <i>(Multiple answers are possible)</i></p>	<p><input type="checkbox"/> () Responsible persons and their duties <input type="checkbox"/> () Preparing for disaster recovery situation <input type="checkbox"/> () Post-disaster recovery tasks <input type="checkbox"/> () Disaster recovery training <input type="checkbox"/> () Disaster Recovery Testing <input type="checkbox"/> () Contact details of external service providers</p>
<p>Confirm that your disaster recovery plans are regularly tested <i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> () We test them at least annually <input type="checkbox"/> () We test them, but less frequently than annually <input type="checkbox"/> () Not tested</p>
<p>Confirm that improvements have been made in test plans due to deficiencies discovered during disaster recovery testing. <i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> () Confirmed <input type="checkbox"/> () No such measures were required <input type="checkbox"/> () Not confirmed</p>
<p>Please specify when the last DRP test was performed</p>	<p>..... (year)</p>
<p>Confirm that their disaster recovery critical workforce has access to all necessary systems. <i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> () Confirmed <input type="checkbox"/> () Not confirmed</p>
<p>Confirm that your organisation has an RTO (Recovery Time Objective) value for CSD relevant processes. <i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> () less than 2 hours <input type="checkbox"/> () Between 2 and 8 hours <input type="checkbox"/> () More than 8 hours</p>

Security management system

<p>Confirm that you have an information security organisation that is independent of other departments.</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> Confirmed</p> <p><input type="checkbox"/> Not confirmed</p>
<p>Does your organisation have a quality assurance certification for information security (e.g.: ISO27001)?</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> Yes If yes, please specify the type, scope and date of certification:</p> <p><input type="checkbox"/> No</p>
<p>Does your organisation have a management-approved information/cyber-security strategy that covers future threats and planned improvements?</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> Yes If so, please provide the date of your last review:</p> <p><input type="checkbox"/> No</p>
<p>Does your organisation have a management-approved information security/cybersecurity policy that includes management's commitment to meeting its security objectives?</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> Yes If yes, please provide the date of entry into force of the current version:</p> <p><input type="checkbox"/> No</p>
<p>Please confirm that your organisation has the following documents:</p> <p><i>(Multiple answers are possible)</i></p>	<p><input type="checkbox"/> Business impact and risk analysis based on international methodology</p> <p><input type="checkbox"/> Business impact analysis updated within one year</p> <p><input type="checkbox"/> Information security risk analysis updated within one year</p> <p><input type="checkbox"/> Action plan or risk list accepted by management</p>
<p>Does your organisation have an information security policy that sets out the duties and responsibilities of users, IT, security, technology controls applied?</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> Yes If yes, please provide the date of entry into force of the current version:</p> <p><input type="checkbox"/> No</p>
<p>Please indicate which of your users have security awareness training for your organisation.</p> <p><i>(Multiple answers are possible)</i></p>	<p><input type="checkbox"/> Security training for new joiners</p> <p><input type="checkbox"/> Annual mandatory security awareness training</p> <p><input type="checkbox"/> Annual mandatory security awareness test</p> <p><input type="checkbox"/> Regular Safety Awareness Newsletter or Tests</p>

<p>Does your organisation have a list of security requirements for system development?</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> Confirmed <input type="checkbox"/> Not confirmed</p>
<p>Frequency of reviewing information security / cybersecurity policies and regulations within the organisation</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> Annually <input type="checkbox"/> Biannually <input type="checkbox"/> If none, please provide frequency:</p>
<p>Confirm that your organization has an up-to-date list of critical service providers.</p>	<p><input type="checkbox"/> Yes If yes, please provide the date of your last review:</p> <p><input type="checkbox"/> No</p>
<p>If you join KELER as a CSD or market infrastructure, please list the critical service providers you have used.⁴</p>	
<p>Does your organisation outsource information security functions or processes?</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> Yes If yes, please identify the security processes, party(ies) involved and specify its headquarter (s).</p> <p><input type="checkbox"/> No</p>

⁴ Pursuant to Article 69 (2) (a) of Commission Delegated Regulation 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 authorisation management system
- Two-factor identification
- Technical user and password management solution

Supervision and audits

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

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

Data centre redundancy

<p>Confirm that you have a backup (secondary) data centre</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> Confirmed Please enter the distance between your data centres (in km): km</p> <p><input type="checkbox"/> Not confirmed</p>
---	---

Backup policy and strategy

<p>Please confirm that your organisation has one of the structured back-up solutions.</p> <p><i>(Multiple answers are possible)</i></p>	<p><input type="checkbox"/> Real time</p> <p><input type="checkbox"/> Mirrored with delay</p> <p><input type="checkbox"/> Daily</p> <p><input type="checkbox"/> Weekly</p> <p><input type="checkbox"/> Other</p>
---	--

Capacity management

<p>Confirm that your organisation has capacity management.</p> <p><i>(Only one answer is possible)</i></p>	<p><input type="checkbox"/> A capacity plan, supported with monitoring system and historical data, is prepared at least once a year</p> <p><input type="checkbox"/> There is only a monitoring system</p> <p><input type="checkbox"/> Not confirmed</p>
--	---

III.4 Operation questions

<p>Please provide the average number of daily transactions you are expected to submit annually on paper</p>	
<p>How many of the average daily expected paper-based transactions are expected to be in EUR currency, DVP settlement, affecting the Hungarian market.</p>	
<p>Please indicate the currencies in which you plan to make settlement.</p>	
<p>Is your organisation ready to communicate via SWIFT and / or KID (KELER Interface Device - KELER's own online system)? If not, how do you envisage communication?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No, we envisage communication as follows:</p>

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 organisation I represent.

Client / Organisation name

Respondent's name, position, contact details (e-mail/phone)

(Authorised signatory's name)

(Position)

(Organisation name)

(Authorised signatory's name)

(Position)

(Organisation name)

(Place): _____, (date): _DD/MM/YYYY_____