KELER Depository Announcement – No. 9-10

on the procedures to inform Clients securely in the case of fraud or security threats perceived or detected by KELER Ltd.

Effective from: 9 February 2021

This Depository Announcement includes information on the procedure to inform Clients securely in the case of fraud or security threats perceived or detected by KELER Ltd.

KELER Group applies various tools and methods in connection with internal controls and (information) security from its existing toolkit for the prevention of abuses and different security threats.

a) Information security tools and methods

- Physical security
- Network security
- Endpoint security
- Data security
- Identity and access management
- Data centre and server security
- Security monitoring and incident response
- Security training
- Regulation/compliance (regulation/security compliance (audits, penetration tests)/BCP-DRP)

b) Internal control tools and methods

- operation of internal control system (for instance four-eye principle),
- preliminary and subsequent executive audits, and executive audits built into the process,
- independent internal audit activity,
- compliance activity,
- appropriate substitution system,
- whistleblowing system,
- strict regulation of personal transactions (Regulation on Conflict of Interest, prohibition of transactions involving internal information).

If KELER Ltd. incidentally perceives or detects fraud or security threats, in the interest of secure use, KELER informs Clients on the security procedure it introduces and/or the security procedure it expects from Clients (users), in due course, as follows:

1. If the group of Clients involved can be defined well, information is sent electronically to the user e-mail address provided upon contracting, and, depending upon the severity of the case, KELER attempts to provide information at the user phone number provided upon contracting.
2. If a large number of Clients is involved, KELER Ltd. publishes information on its website and in the announcement published in the KID (KELER Interface Device) system. Additionally, if justified, KELER informs Clients in e-mail, at the user e-mail address provided upon contracting.

Clients are required to monitor regularly the above information provided on the website of KELER Ltd. (https://english.keler.hu) and in the KID system, and act accordingly.

KELER Ltd. does not request its Clients to provide passwords, login codes or other confidential data via email or text message or by phone for any purpose.

It is important that you should not share your personal data, identifiers, passwords and login codes under any circumstances.

KELER Ltd. does not assume any responsibility for damage resulting from inappropriate use, e.g. from failure to keep username and password login code secret.

Budapest, 2 February 2021

KELER Ltd.