Privacy Notice on the Processing of Data and Copies of Documents Provided in Relation to the Prevention of Money Laundering

1. What is the purpose of this Privacy Notice?

The purpose of this Privacy Notice is to provide the natural persons concerned (the "Data Subject") with detailed and comprehensible information about the processing of data and copies of documents provided in connection with the prevention of money laundering in order to fulfil the obligations prescribed by Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (the "Act on AML").

2. Who are the Controllers?

The Controllers are:

- Ernst & Young Kft. (registered office: 1132 Budapest, Váci út 20.)
- Ernst & Young Tanácsadó Kft. (registered office: 1132 Budapest, Váci út 20.)
- Vámosi-Nagy Ernst & Young Ügyvédi Iroda (registered office: 1132 Budapest, Váci út 20.)

together, the "Controllers".

The Controllers determine the purposes and means of processing personal data. The Controllers process the Data Subjects' personal data lawfully, fairly and transparently, for specified purposes and limited to what is necessary.

The Controllers do not carry out automated processing or profiling in relation to the processed data.

The contact details of the Controllers' data protection officer: dr. Dániel Kokas DPO data.protection@hu.ey.com.

3. For what purposes do the Controllers process personal data?

The processing is required by Section 7(8) of the Act on AML for the purposes of preventing and combating money laundering and terrorist financing, properly fulfilling the obligations set out in the Act on AML, fully carrying out the customer due diligence obligation and effectively performing supervisory activities.

If the Data Subject does not provide the necessary personal data, the Controllers cannot establish the business relationship, cannot execute the transaction order or must terminate any business relationship already established.

4. What is the legal basis for the processing and on what basis do the Controllers process personal data?

The processing is necessary for compliance with a legal obligation to which the Controllers are subject (Article 6(1)(c) GDPR), as this processing is based on an obligation prescribed by the Act on AML. The Controllers process personal data on the basis of Section 7(8a) and Section 56 of the Act on AML.

5. How long do the Controllers process your personal data?

The Controllers are required to keep records in a retrievable and verifiable manner and to retain for 8 years following termination of the business relationship, or performance or termination of the transaction order, the personal data obtained in the course of fulfilling obligations set out in the Act on AML and in legislation based on its authorisation.

The Controllers are required to delete or destroy the data, document or copy thereof without delay after expiry of the retention period, unless the Office Against Money Laundering and Terrorist Financing, investigating authority, public prosecutor's office or court has instructed the Controllers in its request to extend the retention period. In this case, the retention period may be a maximum of 10 years following termination of the business relationship if those authorities need the data, documents or copies of documents processed by the Controllers to conduct ongoing proceedings or proceedings to be commenced in the future.

6. How do the Controllers ensure that your personal data are secure?

The Controllers protect the personal data processed against unauthorised access, alteration, transfer, disclosure, erasure, damage or destruction through appropriate technical and organisational measures.

The Controllers restrict access to personal data, treat the data confidentially and ensure that persons involved in processing act subject to appropriate confidentiality and data protection obligations. Where personal data are transferred within the Controllers' network, the Controllers ensure the applicable data protection safeguards, among other things, on the basis of the Controllers' binding corporate rules. Further information on the Controllers' BCR programme is available here: https://www.ey.com/en_gl/legal-and-privacy/data-protection-binding-corporate-rules-program.

7. What should you do if you have a question or problem concerning the processing?

You have the right to request information as to whether the Controllers process personal data relating to you and, if so, to obtain access to the relevant data and information about the processing. You may verify that your personal data are accurate and up to date.

You have the right to request the rectification of inaccurate personal data, the completion of incomplete data and, where the conditions set out in the GDPR are met, the erasure of or restriction of processing of your personal data, and you may object to the processing of your personal data.

If you believe that the processing of your personal data infringes the applicable data protection legislation, you may lodge a complaint with the National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa utca 9-11.; telephone: +36 1 391 1400; e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu), or you may initiate court proceedings.

The Controllers will respond to requests received from Data Subjects without undue delay and no later than one month from receipt of the request. Where necessary, taking into account the complexity and number of requests, this period may be extended by a further two months.

8. Transfers of personal data to other countries

The Controllers' member firms operate in more than 150 countries worldwide. Certain elements of the Controllers' operations are centralised, including IT services provided to member firms. In addition, where the Controllers' client engagements involve more than one jurisdiction, certain information must be accessible within the Controllers' organisation to all employees working on the engagement. For this reason, the Data Subject's personal data are transferred by the Controllers to, and stored in, countries outside the Data Subject's place of residence. These include countries outside the European Economic Area (EEA) and countries whose laws do not necessarily ensure an adequate level of protection for the processing of personal data under the laws of the EU or other jurisdictions.

The Controllers take all appropriate security and legal precautions within their organisation to ensure the security and integrity of the personal data transferred. The Controllers have implemented binding corporate rules enabling the international transfer within the EY organisation of personal data originating in the EEA in accordance with European data protection laws. The binding corporate rules require all member firms of the Controllers worldwide to protect personal data to the same level. Their binding corporate rules are available in English here.

9. Who may access your personal data?

9.1. Within the EY organisation

Employees, agents or other persons acting on behalf of the Controllers may access your personal data where this is necessary for the performance of their duties.

9.2. Transfer of personal data to third-party service providers

The Controllers may transfer the personal data they collect to third-party service providers (and their subsidiaries and affiliates) engaged by the Controllers to support internal auxiliary processes. The Controllers may therefore engage service providers to provide, operate and support IT infrastructure (such as identity management, hosting, data analysis, backup, security and cloud storage services), and to store and securely destroy printed documents.

The Controllers use only third-party service providers that are required to maintain an appropriate level of data protection, security and confidentiality.

The further content of this Privacy Notice is drafted separately for each type of form, uniformly for all Controllers.

I. <u>CLIENT IDENTIFICATION SHEET (Natural person)</u>

What personal data do the Controllers process?

The personal data of the natural-person client are: full name (name used), full name at birth, mother's maiden name, place and date of birth, nationality, type and number of photographic identity document, place of residence or, in the absence thereof, place of stay, position, politically exposed person (PEP) status and type thereof.

If acting in the name or on behalf of another beneficial owner or beneficial owners, the natural-person client must declare the following personal data of the beneficial owner or beneficial owners: surname and given name, surname and given name at birth, nationality, place and date of birth, address or, in the absence thereof, place of stay, nature of the ownership interest, politically exposed person (PEP) status and type thereof.

In addition, where politically exposed person status exists, the declaration must state the lawful source of the funds. A supporting document must be attached, which requires the processing of personal data contained in the following documents:

- data contained in a certificate of salary income from employment;
- data contained in a certificate of income received for service abroad;
- data in a certificate relating to capital gains, prizes or dividends;
- where the funds originate from inheritance, compensation or civil-law relationships, data in the related agreement or official document;
- data contained in another certificate of income.

The Controllers also process the following personal data:

- Name and signature of the Data Subject completing the declaration

II. <u>CLIENT IDENTIFICATION SHEET (In the case of a legal person):</u>

What personal data do the Controllers process?

If applicable, the full name and place of residence or, in the absence thereof, place of stay of the client's delivery agent.

The client's representative: full name, full name at birth, mother's maiden name, place and date of birth, nationality, designation and number of photographic identity document, place of residence or, in the absence thereof, place of stay, and position.

The beneficial owner as defined in Section 3(38)(a)-(g) of the Act on AML: surname and given name, surname and given name at birth, nationality, place and date of birth, address or, in the absence thereof, place of stay, ownership interest and the extent thereof, politically exposed person (PEP) status and type thereof.

In addition, where politically exposed person status exists, the legal person must state the lawful source of the funds in a declaration. A supporting document must be attached, which requires the processing of personal data contained in the following documents:

- data contained in a certificate of salary income from employment;
- data contained in a certificate of income received for service abroad;
- data in a certificate relating to capital gains, prizes or dividends;
- where the funds originate from inheritance, compensation or civil-law relationships, data in the related agreement or official document;
- data contained in another certificate of income.

The Data Subject must also attach additional documentary annexes to the document, meaning that the Controllers also process personal data appearing on the following documents:

<u>In the case of a representative and/or beneficial owner of a legal-person (or entity without legal personality) client:</u>

- if the Data Subject is a Hungarian citizen: identity card, passport or card-format driving licence, the page of the address card that does not contain the personal identification number, if the place of residence or place of stay is in Hungary, and power of attorney (if the person is not a representative authorised to sign for the company)
- if the Data Subject is a foreign citizen: passport or identity card, provided that it entitles the holder to stay in Hungary, or a document certifying the right of residence or a document entitling the holder to stay, the page of the address card that does not contain the personal identification number, if the place of residence or place of stay is in Hungary, and power of attorney (if the person is not a representative authorised to sign for the company)

<u>In the case of a private investment fund client:</u>

- the private investment fund's fund rules and instrument of incorporation,
- a document concerning the fund's capital (the aggregate capital contributions) and the ratio of each investor's capital interest,
- a document supporting the identity of the investors – in particular, whether they are professional or retail investors – and the rights and obligations of the investors as set out in the fund rules, as well as the material obligations arising from the fund manager's legal representative status.

The Controllers also process the following personal data:

- name and signature of the Data Subject completing the declaration

III. DECLARATION OF POLITICAL EXPOSURE (PRIVATE INDIVIDUAL)

What personal data do the Controllers process?

The personal data of the private individual making the declaration are: name, place and date of birth, address, politically exposed person (PEP) status and type thereof.

In addition, where politically exposed person status exists, the declaration of political exposure must state the lawful source of the funds. A supporting document must be attached, which requires the processing of personal data contained in the following documents:

- data contained in a certificate of salary income from employment;
- data contained in a certificate of income received for service abroad;
- data in a certificate relating to capital gains, prizes or dividends;
- where the funds originate from inheritance, compensation or civil-law relationships, data in the related agreement or official document;
- data contained in another certificate of income.

The Controllers also process the following personal data:

- name and signature of the Data Subject completing the declaration of political exposure

IV. DECLARATION OF POLITICAL EXPOSURE (REPRESENTATIVE)

What personal data do the Controllers process?

The representative of the client legal person: full name, full name at birth, mother's maiden name, place and date of birth, nationality, designation and number of photographic identity document, place of residence or, in the absence thereof, place of stay, and position.

The beneficial owner as defined in Section 3(38)(a)-(g) of the Act on AML: name, place and date of birth, address, politically exposed person (PEP) status and type thereof.

In addition, where politically exposed person status exists, the declaration of political exposure by the representative must state the lawful source of the funds. A supporting document must be attached, which requires the processing of personal data contained in the following documents:

- data contained in a certificate of salary income from employment;
- data contained in a certificate of income received for service abroad;
- data in a certificate relating to capital gains, prizes or dividends;

- where the funds originate from inheritance, compensation or civil-law relationships, data in the related agreement or official document;

- data contained in another certificate of income.

The Data Subject must also attach additional documentary annexes to the document, meaning that the Controllers also process personal data appearing on the following documents:

<u>In the case of a representative and/or beneficial owner of a legal person client:</u>

- if the Data Subject is a Hungarian citizen: identity card, passport or card-format driving licence, the page of the address card that does not contain the personal identification number, if the place of residence or place of stay is in Hungary, and power of attorney (if the person is not a representative authorised to sign for the company)

- if the Data Subject is a foreign citizen: passport or identity card, provided that it entitles the holder to stay in Hungary, or a document certifying the right of residence or a document entitling the holder to stay, the page of the address card that does not contain the personal identification number, if the place of residence or place of stay is in Hungary, and power of attorney (if the person is not a representative authorised to sign for the company)

<u>In the case of a private investment fund client:</u>

- the private investment fund's fund rules and instrument of incorporation,
- a document concerning the fund's capital (the aggregate capital contributions) and the ratio of each investor's capital interest,
- a document supporting the identity of the investors – in particular, whether they are professional or retail investors – and the rights and obligations of the investors as set out in the fund rules, as well as the material obligations arising from the fund manager's legal representative status.

The Controllers also process the following personal data:

- name and signature of the Data Subject completing the declaration of political exposure by the representative