

# **FREEDOM FINANCE EUROPE LTD**

## **DATA PROTECTION POLICY**

23<sup>rd</sup> of November 2023

Name of document: **Data Protection Policy**

Type of document **Internal Policy**

### Version History

Version	Date of update	Reason of update	Date of approval	Remarks
1.0	25.05.2018	Data protection notice	-	n/a
2.0	10.08.2022	Change of format	17.10.2022	n/a
3.0	23.11.2023	Annual Review	30.11.2023	No changes

## Contents

1. Introduction.....	4
2. Definitions.....	4
3. Scope and purpose .....	5
4. General principles.....	6
5. Obligations and responsibilities .....	8
6. Legal basis for personal data processing .....	9
7. Processing operations and means .....	10
8. Categories of personal data recipients .....	10
9. Data subject rights.....	11
10. Period for which the personal data is stored.....	14
11. Personal data provision requirements .....	15
12. Change of terms and conditions of data processing.....	16
13. Policy review .....	16
Annex 1. Purposes of and legal basis for personal data processing.....	17

## 1. Introduction

1.1. Freedom Finance Europe Limited (hereinafter called the “Company”) is a Cypriot Investment Firm (“CIF”) registered with the Registrar of Companies under number HE 324220 and regulated by the Cyprus Securities & Exchange Commission (“CySEC”) under license number 275/15.

1.2. Following the requirements and/or obligations implemented by the following laws and regulations and in compliance with the current legal framework:

- The General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
- Directive 95/46/EC (General Data Protection Regulation)
- Data Protection Act 2018 125(I)/2018 of 31 July 2018 for the protection of natural persons with regard to the processing of personal data and for the free movement of such data

the Company shall develop an adequate Data Protection Policy that is adopted by the Board of Directors and communicated to everyone involved, including the customers of the Company, to ensure their commitment to it.

## 2. Definitions

2.1. **Client / Customer** refers to any person from whom, or on whose behalf, the Company receives, acquires or holds funds or securities for such person’s account.

2.2. **Personal data** means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- 2.3. **Data processing** means any operation or set of operations that is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 2.4. **Data subject** is an individual who is the subject of personal data. This includes partnerships and groups of individuals but is not limited to companies. In terms of this Policy, all customers and employees are data subjects.
- 2.5. **Data controller** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and how any personal data are or are to be processed.
- 2.6. **Data processor** refers to any person (other than an employee of the Company) who processes the data on behalf of the Company.

### 3. Scope and purpose

- 3.1. The purpose of the present Data Protection Policy is to provide information on the terms and conditions of the processing of personal data and special categories of personal data by Freedom Finance Europe Ltd (hereafter “the Company”) as required under General Data Protection Regulations (GDPR) and relevant Cyprus laws and Acts.
- 3.2. The main purposes of personal data processing are as follows:
- a) conclusion/performance of a contractual relationship where the client is a party;

- b) compliance with legal obligations to which the Company is subject under Union laws or Member State laws;
- c) legitimate interests pursued by the Company or by a third party (including but not limited to compliance with foreign regulatory requirements, conclusion and/or performance of contracts, marketing (including direct marketing) of financial products and services, and products and services associated with them (trading platforms, market data services, etc.), security, establishment, exercise or defense of legal claims).

3.3. The Company is entitled to process personal data for purposes other than specified herein with prior notification to the Client.

3.4. The purposes of and legal basis for personal data processing are described in Annex 1 hereto.

3.5. The Policy covers both personal and special categories of personal data (as defined by Article 4 of the GDPR) held in relation to data subjects by the Company.

3.6. The Policy applies to personal data held in both manual and automated forms. Unless expressly stated otherwise, both categories will be equally referred to as Personal Data in this Policy. Personal data and special categories of personal data will be treated with equal care by the Company.

#### **4. General principles**

4.1. The Company shall process personal data related to natural persons who are the clients and/or potential clients of the Company, clients' representatives, decision-makers, directors, beneficial owners, controlling persons of legal entities (hereafter the "Data Subject", "Client" and/or "Customer").

4.2. Personal data include all personal data received by the Company from its clients, third persons or publicly accessible or available sources on a proper legal basis, including but not limited to the data specified in the questionnaires and other fill-in forms, data

on property, property rights and liabilities, data of contracts (including names, numbers, and conclusion dates), data on the accounts opened with the Company or third parties, data on transactions and other operations performed by the clients or on behalf or for the benefit of the clients as well as the specified (updated, amended) data received by the Company subsequently.

4.3. All personal data processing shall be conducted in accordance with the data protection principles set out in relevant legislation. The Company's policies and procedures are designed to ensure compliance with the following principles:

- **Lawfulness, fairness and transparency:** personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
- **Purpose limitation:** personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be inconsistent with the initial purposes in accordance with Article 89(1)
- **Data minimization:** personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **Accuracy:** personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- **Storage limitation:** personal data shall be kept in a form that permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to the implementation

of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject

- **Integrity and confidentiality:** personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures

## 5. Obligations and responsibilities

- 5.1. The Company is committed to complying with all the relevant EU and the Republic of Cyprus laws, together with the laws of other Member States where its representative offices are located, related to personal data, and the protection of the rights and freedoms of individuals whose information the Company may possess, control and/or process.
- 5.2. The Company shall implement appropriate technical and organizational measures to ensure that processing is performed in accordance with the GDPR.
- 5.3. All the Company employees collecting and/or controlling the content and the use of personal data are responsible for ensuring personal data is collected, stored and handled appropriately.
- 5.4. Each Department that handles and/or has access to personal data must ensure that data will be handled and processed in line with this Policy, best practice and data protection legislation.
- 5.5. The Company has appointed Oleg Tupiko as an internal Data Protection Officer (hereafter DPO) as required under Article 37 of the GDPR. The DPO is an independent function and will not receive instructions from other managers regarding exercising the designated DPO tasks and duties. The Company's Data Protection Officer's contact information is as follows:



Address: Christaki Kranou 20, Freedom Tower, Germasogeia, 4041, Limassol, Cyprus

Phone: +357 25257787

Data Protection Officer: Oleg Tupiko

E-mail: [dpo@ffineu.eu](mailto:dpo@ffineu.eu)

5.6. All the employees of the Company have the responsibility to comply with the provisions of the present Data Protection Policy.

## 6. Legal basis for personal data processing

6.1. Below are the rights the client is entitled to when his/her personal data is processed for the purpose and on the legal basis of the legitimate interests pursued by the controller or by a third party:

- **Right to receive additional information:** to rely on legitimate interests as a lawful basis for personal data processing, the Company must carry a balancing test to ensure that these legitimate interests are not overridden by the client's interests or fundamental rights and freedoms that require protection of personal data. The Company can provide information from the balancing test on the client's request.
- **Right to object:** Where the data processing is based on the legitimate interests pursued by the Company or by a third party the client is entitled to object to such processing. The client is entitled to object against processing for the purpose of direct marketing and in case of such written objection from the client, the Company shall terminate the processing for this purpose unconditionally. For more information about the right to object, please, refer to Section "Right to object" of Article 21 of GDPR.

## **7. Processing operations and means**

- 7.1. Processing operations consist of collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing, destroying, or any other operations for the purposes and principles of data processing.
- 7.2. Personal data may be processed by automated or not automated means.

## **8. Categories of personal data recipients**

- 8.1. The following categories of persons are among the possible recipients of personal data:
- third persons involved in the Data Subject's services such as brokers, custodians, depositaries, banks, trading venues including third-country trading venues, software and market data providers, EU and third countries competent authorities
  - any person authorized to audit or conduct a similar control of the Company or third persons involved in the Data Subject's servicing and marketing located both in EU and non-EU countries.
- 8.2. Most non-EU countries are not recognized by European Commission as countries ensuring an adequate level of personal data protection by adopting the relevant decision (hereinafter referred to as an “adequacy decision”). Under GDPR, personal data to such countries may be transferred under the condition that appropriate safeguards are provided or in the absence of such safeguards under conditions specified in Article 49 of GDPR.
- 8.3. The Company may transfer personal data to service providers in third countries which have appropriate safeguards in place.
- 8.4. Appropriate safeguards mentioned above without requiring any specific authorization

from a supervisory authority are:

- a) legally binding and enforceable instrument between public authorities or bodies;
- b) binding corporate rules in accordance with Article 47 of GDPR;
- c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) of GDPR;
- d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) of GDPR;
- e) an approved code of conduct pursuant to Article 40 of GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including client's rights; or
- f) an approved certification mechanism pursuant to Article 42 of GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including client's rights.

## 9. Data subject rights

9.1. Any Company's client is entitled to the rights specified herein only in the scope of GDPR. Rules applicable to personal data processing in third countries may significantly differ, and the person may not be entitled to rights equivalent to those established by GDPR or such rights may be limited.

9.2. **Right to withdraw consent for the data processing:** Where the personal data processing is based on the data subject consent, the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Regarding relations between the client and the Company, such right may be executed by sending a duly signed notice in writing by fax, email, post or delivery of such information in person. A natural person whose e-mail address was provided by filling the relevant form may also be used for the aforementioned right by sending a duly signed soft copy of the relevant notice by email from the e-mail provided to the Company. Such right

may be executed within five (5) years from the end of the relationships with the relevant natural person.

- 9.3. **Right of access:** Any client shall have the right to obtain confirmation as to whether or not personal data concerning him/her are being processed, and, when that is the case, access to the personal data, a copy of the personal data undergoing processing and the information concerning the processing of his/her personal data. When a client makes a request by electronic means, and unless otherwise requested, the information shall be provided in a commonly used electronic form.
- 9.4. **Right to rectification:** The Data Subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him/her. Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- 9.5. **Right to erasure ('right to be forgotten):** A client shall have the right to obtain from the Company the erasure of personal data concerning him/her without undue delay and the Company shall have the obligation to erase personal data without undue delay under conditions as specified in Article 17 of GDPR. Please note that this right shall not be adequate to the extent that processing is necessary for the purposes stipulated in Article 17 of GDPR, in particular, for compliance with a legal obligation that requires processing by Union or Member State law to which the controller is subject.
- 9.6. **Right to restriction for processing:** A client shall have the right to obtain from the Company the restriction for processing where one of the following applies:
- i) the accuracy of personal data is contested by the client for a period enabling the Company to verify the accuracy of the personal data;
  - ii) the processing is unlawful, and the client opposes the erasure of the personal data and requests the restriction of their use instead;
  - iii) the Company no longer needs the personal data for the purposes of the processing but is addressed by the client for the establishment, exercise or defense of legal claims;

- iv) a client has objected to processing pursuant to Article 21(1) of GDPR pending the verification of whether the legitimate grounds of the Company override those of the client.

Where processing has been restricted under Article 18 of GDPR, such personal data shall, with the exception of storage, only be processed with the client's consent, or for the establishment, exercise or defense of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or a Member State.

**9.7. Right to data portability:** A client shall have the right to receive the personal data concerning him/her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- i) the processing is based on consent pursuant to point (a) of Article 6(1) of GDPR or on a contract pursuant to point (b) of Article 6(1) of GDPR; and
- ii) the processing is carried out by automated means.

**9.8. Right to object:** A client will have the right to object, on grounds relating to a particular situation, at any time to the processing of personal data concerning him/her which is based on point (f) of Article 6(1) of GDPR. The Company shall no longer process client's personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the client or for the establishment, exercise or defense of legal claims. Where personal data are processed for direct marketing purposes, a client will have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where a client objects to processing for direct marketing purposes, his/her personal data will no longer be processed for such purposes. Please pay attention that when a client objects to processing for the purpose of direct marketing the Company shall terminate processing for such purpose unconditionally unlike data processing for other legitimate interests

where the Company may continue further processing provided that it has demonstrated compelling legitimate grounds.

9.9. **Right to lodge a complaint with a supervisory authority:** Without prejudice to any other administrative or judicial remedy, every data subject will have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes GDPR.

## 10. Period for which the personal data is stored

10.1. The Company shall retain the personal data processed for as long as it is considered necessary for the purpose for which it is processed (including as required by applicable law or regulation).

10.2. Considering the general limitation period stipulated by the Republic of Cyprus laws and in the absence of specific regulatory or contractual requirements, the Company's baseline retention period for the personal data is seven (7) years. Where the same personal data is processed for different purposes, the storage period is determined by the purpose for which a longer period is necessary. Considering the "storage limitation" principle stipulated by Article 5 of GDPR and specific circumstances related to the personal data the Company may retain the personal data for the period less than the baseline retention period.

10.3. Below, you will find the main requirements concerning the retention of personal data relating to the Company's processing operations:

- i. EU and the Republic of Cyprus laws regarding the provision of investment services – five (5) years;
- ii. Prevention of money laundering and financing terrorism legislation – five (5) years from the end of the Controller's relationship with the client or from the date of the last carried-out transaction;

- iii. FATCA – six (6) years starting from the end of the year when FATCA status of the client is identified;
- iv. CRS – six (6) years from the moment of identification of the country where the client or its controlling persons are tax residents.
- v. EU directive 565/2017 – telephone communications between the CIF and its clients are recorded, and a copy of the recording of such communications with the client will be available on request for a period of five (5) years and where requested by the competent authority, for a period of up to seven (7) years.
- vi. CY Directive L. 87(1)/2017 – telephone communications or conversations between the CIF and its clients that result or may result in transactions will be recorded and collected for a period of five (5) years, even if those conversations or communications do not result in the conclusion of such transactions or the provision of client order services.

## **11. Personal data provision requirements**

11.1. Most personal data is provided by filing an application form and the content of the information required for different purposes coincides.

11.2. For example, the name of the client is required both for compliance with AML legislation and for the conclusion/performance of the contract. Another example is the tax residence of the client, which is required for compliance with FATCA, and CRS requirements and for the performance of the contract to ensure the receipt of the proper amount of distribution paid on securities held on the client's account opened with us.

11.3. Therefore, as it follows from the examples in many cases the same data is provided under statutory requirements, contractual requirements and requirements necessary to enter into a contract.

11.4. The possible consequence of failure to provide such data is the Company's refusal to conclude the contractual relationship or the termination of the contractual relationship concluded with the client.

11.5. If you have any query concerning requirements for the provision of specific data, please

contact us using the contact details provided herein.

## **12. Change of terms and conditions of data processing**

12.1. The terms and conditions of data processing may be changed by the Company unilaterally by posting the new version of the Data Protection Policy/Notice on any of its official websites:

- <https://freedomfinance.eu/>
- <https://freedom24.com/>

## **13. Policy review**

13.1. The present Policy shall be reviewed annually or whenever a material change occurs that affects the Company's procedures and principles related to data protection obligations and requirements.



### Annex 1. Purposes of and legal basis for personal data processing

No.	Personal data / Specific operation	Purpose	Legal basis (in accordance with Art. 6 of GDPR)
1	Data as specified in the form and Form W8BEN, data obtained as a result of the acceptance and performance of the contractual relationship specified in Terms and Conditions for the provision of investment and ancillary services of the Controller and other agreements and contracts associated with the conclusion and performance of the contractual relationship on details of the contract, transactions and other operations made via and with the Controller.	Conclusion/performance of a contract where the Subject is a party (Agreement for the provision of investment and ancillary services concluded between the Subject and the Controller and other agreements and contracts associated with the conclusion and performance of the Agreement).	Processing is necessary for the performance of a contractual relationship to which the Data Subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
2	Personal data as required under the relevant Union law or Member State law to which the Controller is subject.	Compliance with a legal obligation to which the Controller is subject under Union law or Member State law (Prevention of money laundering and financing terrorism legislation; MIFID II, MIFIR, Law 87(I)/2017 regarding the provision of investment services, the exercise of investment activities and the operation of regulated markets and other Union and Member State laws regulating provision of investment services, the exercise of investment activities and the operation of regulated markets, Market Abuse legislation, FATCA and CRS as implemented in Cyprus and European Union, the United States, United Kingdom or Member State laws as may be applicable).	Processing is necessary for compliance with a legal obligation to which the controller is subject under European Union, the United States, United Kingdom or Member State laws.

3	<p>Personal data as required under applicable foreign regulatory requirements/contracts or as nature of the relevant legal claim may require.</p>	<p>Legitimate interests of the Controller or a third party involved in the provision of services to the client (intermediate broker, depositary, custodian, bank) to comply with the foreign regulatory requirements (in particular, laws of the United States of America, United Kingdom, CIS countries, or other countries (as may be applicable to you) concerning taxation of income paid or credited to the client's the account, FATCA – the US law which has extraterritorial application and where it is applied in the third country to the extent admitted in that third country). Legitimate interests of the Controller to comply with tax laws of the United States of America. Legitimate interests of the Controller and or a third party to conclude and perform the contracts associated with the provision of the Controller investment and ancillary services. The aforementioned shall not include cases where the processing of personal data under the relevant regulatory requirements/contracts is required for the purpose of conclusion/performance of a contractual relationship with the Data Subject and consequently such processing falls under the legal basis specified in item 2 above. Legitimate interests of the Controller and third parties associated with the establishment, exercise or defense of legal claims (potential legal claims) arising from or in connection with the provision of services by the Controller.</p>	<p>Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. The legitimate interests are identified in the second column of this table.</p>
4	<p>Contact details, including email and names.</p>	<p>Marketing (including direct marketing) of financial products and services and products and services associated with them (trading platforms, market data services, etc.).</p>	<p>The Data Subject has given consent to the processing of the personal data for these purposes.</p>

5	<p>Transfer of the Client's personal data to third countries which are not recognized by the European Commission as countries ensuring an adequate level of personal data protection by adopting a relevant decision for the purpose specified in the second column of this table. Personal data to be transferred: personal data as required to provide compliance with FATCA (including but not limited to name, citizenship, address, tax residence, place and date of birth, taxpayer identification number, information regarding account(s) opened with the Company, account(s) balance, income paid or credited to the account(s) with the Company and gross proceed from the sale or other distribution of financial assets credited to the account(s) with the Company, taxes withheld from income paid or credited to the account(s) with the Company). Personal data may be transferred in whole or in part by the provision of the Self-Certification form contained herein or/and W -8BEN form or by submitting reports on Form 1042 -S.</p>	<p>Provision of FATCA compliance by the Company's and any person that has control, receipt, or custody of income or that can disburse or make payments of income (where FATCA applied out of scope of FATCA Intergovernmental Agreement between Cyprus and the USA)</p>	<p>The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes. This legal basis shall not be applicable where the transfer is necessary for the performance of a contractual relationship between the Data Subject and the Company or the implementation of pre-contractual measures taken at the Data Subject's request or for the conclusion or performance of a contractual relationship concluded in the interest of the data subject between the Company and another natural or legal person (e.g., provision of information by the Company to the custodian/depositary where the Client's financial instruments are held or intended to be held). In such cases, personal data could be transferred irrespective of the Client's consent.</p>
6	<p>Personal data as required under the relevant European Union, the United States, United Kingdom or Member State law to which the Controller is subject</p>	<p>Compliance with a legal obligation to which the Controller is subject under Union law or Member State law (Prevention of money laundering and financing terrorism legislation; MIFID II, MIFIR, Law 87(I)/2017 regarding the provision of investment services, the exercise of investment activities and the operation of regulated markets and other Union and Member State laws regulating provision of investment</p>	<p>Personal data as required under the relevant European Union, the United States, United Kingdom or Member State law to which the Controller is subject</p>

		<p>services, the exercise of investment activities and the operation of regulated markets, Market Abuse legislation, FATCA and CRS as implemented in Cyprus and Union or Member State laws as may be applicable).</p>	
<p>7</p>	<p>Personal data as required under applicable foreign regulatory requirements/contracts or as the nature of the relevant legal claim may require.</p>	<p>Legitimate interests of the Controller, the Data Subject or a third party to conclude and perform the following contracts: Agreement for the provision of investment and ancillary services between the Data Subject and the Controller and other agreements and contracts associated with the conclusion and performance of the Agreement, Contracts concluded between the Controller and third persons involved in the Data Subject's services such as brokers, custodians, depositaries, banks, trading venues including third-country trading venues, software and market data providers. Legitimate interests of the Controller or a third party involved in the provision of services to the Data Subject (intermediate broker, depositary, custodian, bank) to comply with the foreign regulatory requirements (in particular, laws of the United States of America, United Kingdom, CIS countries, or other countries (as may be applicable to you) concerning taxation of income paid or credited to Data Subject's the account, FATCA - US law which has extraterritorial explication and where it is applied in the third country to the extent admitted in that third country). Legitimate interests of the Controller and third parties associated with the establishment, exercise or defense of legal claims (potential legal claims) arising from or in connection with the provision of services by the Controller.</p>	<p>Personal data as required under applicable foreign regulatory requirements/contracts or the as nature of the relevant legal claim may require.</p>

8	<p>Transfer of the Data Subject's personal data to third countries not recognized by the European Commission as countries ensuring an adequate level of personal data protection by adopting a relevant decision without appropriate safeguards. The personal data shall be transferred to the extent necessary for the achievement of the relevant purposes.</p>	<p>Legitimate interests as specified in point 2.1. above except legitimate interests in relation to legal claims as the transfer for the establishment, exercise or defense of legal claims is allowed under Article 49 of GDPR.</p>	<p>The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes.</p>
9	<p>Personal data as required under the relevant Union law or Member State law to which the Controller is subject.</p>	<p>Compliance with a legal obligation to which the Controller is subject under Union law or Member State law (Prevention of money laundering and financing terrorism legislation; Market Abuse legislation and other Union or Member State laws as may be applicable).</p>	<p>Processing is necessary to comply with a legal obligation to which the controller is subject under Union or Member State law.</p>
10	<p>Personal Data as may be required for relevant purposes.</p>	<p>Conclusion/performance of a contract where the Data Subject (Donee) is a party (Agreement for the provision of investment and ancillary services between the Data Subject and the Controller and other agreements and contracts associated with the conclusion and performance of the contractual relationship). Legitimate interests of the Controller and third parties related to the establishment, exercise or defense of legal claims (potential legal claims) arising from or in connection with the provision of services by the Controller.</p>	<p>Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. The legitimate interests are identified in the second column of this table.</p>