

EURONEXT SECURITIES COPENHAGEN

Rule Book – Part 7 Name Registration Service Rules

Date: [***] 2026

1. Scope

- 1.1. These Name Registration Service Rules being Part 7 of the VP Rule Book apply to the Name Registration Services (as described below) and apply in addition to the terms and conditions contained in Part 1 to 6 of the VP Rule Book to Issuers and Participants that participate in the additional service, Name Registration Services.
- 1.2. In the event of any inconsistency between the Name Registration Service Rules and other parts of the Participation Agreement, the Name Registration Service Rules shall prevail.
- 1.3. Terms defined in Part 1 of the VP Rule Book (Definitions) have the same meaning when used in the Name Registration Service Rules, unless otherwise stated herein or the context otherwise requires.

2. Description of the Name Registration Services

- 2.1. The purpose of the Name Registration Services is to support Participants, who choose to access the VP system via an omnibus account structure, in maintaining Ownership Information (as defined in clause 5.3) for use in the share register of the Issuer. For securities in omnibus accounts, underlying Ownership Information is not otherwise visible at the level of VP.
- 2.2. The Name Registration Services comprise the following:
 - 2.2.1. VP assisting Participants with name registration of investors in the ownership registers of securities issued in the VP system and in scope (as defined in clause 2.4) for the Name Registration Services by forwarding Ownership Information to the Issuer for effecting, amending and deleting registrations of investors in such ownership register. VP receives the Ownership Information, including CPR, CVR and other personal identification numbers, from the Participants who hold the comprehensive picture of investor holdings connected to Securities Accounts in the VP system. VP then transmits such information as defined in clause 4.1 to the Issuers that participate in the Name Registration Services or their appointed providers of issuer services (referred to as the "Issuer or Relevant Recipient"); and
 - 2.2.2. VP assisting Issuers with identification of their investors in connection with general meetings, voting and the exercise of shareholder rights connected to securities which are in scope for the Name Registration Services. For the purpose of such identification, VP converts the CPR, CVR or other personal identification numbers into investor identification numbers (referred to as "Investor IDs"). CPR, CVR and other personal identification numbers will not be disclosed to the Relevant Recipients but will be kept by VP in accordance with clause 4.4 below.
 - 2.2.3. A service description setting out details of the Name Registration Services is contained in the User Guidelines.
- 2.3. The Name Registration Services are delivered via a dedicated system developed by VP (the "Name Registration System").

- 2.4. The Name Registration Services provided under these Name Registration Service Rules are applicable to all types of securities (equities, bonds, etc.), but only such securities that are issued and Book-entered as Dematerialised Securities in the VP system and in respect of which the Issuer has elected to participate in the Name Registration Services, cf. clause 3.1.
- 2.5. For the avoidance of doubt, VP will continue delivering top-tier account-level information to the Relevant Recipients through the VP system for Securities Accounts maintained in the VP system, where name registration has been requested by the investor or where the name registration is mandatory as set out in the static data.
- 3. Participation in the Name Registration Services**
- 3.1. All securities issued and Book-entered as Dematerialised Securities in the VP system shall be included in the Name Registration Services according to the status set by the Issuing Agent in the static data in the VP system. A change in the registration in the static data (e.g. exemption) takes immediate effect.
- 3.2. To participate in the Name Registration Services the Participant must participate in VP's services as Securities Account Controller and must have signed a Participation Agreement with VP which covers participation in the Name Registration Services. Further, the Participant must agree with VP on which date it wishes to activate the Name Registration Services.
- 3.3. An Issuer may appoint a third-party provider to act on its behalf in relation to the Name Registration Services. The appointed third party may be the Issuer's appointed provider of issuer services. Issuers participating in the Name Registration Services and their appointed third parties are referred to as "Relevant Recipients". Appointment and change of a third-party Relevant Recipient must be agreed with VP and follow the procedure set out in the User Guidelines.
- 3.4. To interact with the Name Registration System, the Participant and/or Issuer must use the technical connection, communication interface, etc. as determined and instructed by VP and as further described in the User Guidelines. This includes populating and signing the VP Name Registration Services SWIFT form appended to the User Guidelines.
- 3.5. The Participant and Issuer each undertake, at their own expense, to develop and implement the systems, processes and connectivity necessary for activating and making use of the Name Registration Services. The User Guidelines set out specific requirements in this regard.
- 3.6. VP has a right to monitor the Participant's and Issuer's access to and use of the Name Registration System.
- 3.7. Each Participant and Issuer must adhere to any technical and operational change instruction from VP, in respect of a change to the Name Registration Services, which VP finds reasonable or necessary to implement. To the extent possible, VP will give the Participant or Issuer (as applicable) due notice of such changes. The Participants and Issuers acknowledge that under certain circumstances, e.g. if it is necessary to ensure the safe and efficient operation

of the Name Registration System, changes may take immediate effect, and each Participant and Issuer must without undue delay adapt to the changes.

- 3.8. Each Participant and Issuer participating in the Name Registration Services must perform all such acts and tests as may be reasonably required by VP. This includes certain tests that must be performed prior to initiation of the Name Registration Services as further described in the User Guidelines. All tests must be performed successfully to a level satisfactory for VP.
- 3.9. The Participant and Issuer might want to perform its own tests, which could require assistance from VP. VP will assist the Participant and Issuer (as applicable) in performing such tests on a best effort basis.
- 3.10. Any intellectual property rights arising from the development or offering of the Name Registration Services shall be owned by VP, regardless of whether a Participant and/or Issuer contributed through testing, providing feedback or otherwise.

4. Rights and obligations of VP

- 4.1. VP shall transmit (i) the Ownership Information set out in clause 5.3 (except from CPR, CVR or other personal identification numbers) received from the Participant and processed by VP and (ii) the related Investor IDs to the Relevant Recipient in accordance with the procedure set out in the User Guidelines.
- 4.2. VP does not verify the accuracy, completeness or validity of the Ownership Information received from the Participant.
- 4.3. VP acts solely as an intermediate provider of Ownership Information to the Relevant Recipient, and does not undertake, and shall not be responsible for, the registration of an investor in the relevant ownership register or for determining whether an investor is entitled to be registered in such ownership register.
- 4.4. Upon instruction from the Participant, cf. clause 5.6, VP shall keep the investors' CPR, CVR or other personal identification numbers, as the case may be, on record for the purpose of maintaining the link between such identification numbers and the corresponding Investor IDs, and for assisting the Relevant Recipient in connection with the exercise of shareholder rights, as described in section 2.2.2.
- 4.5. Subject to retention requirements under applicable law or regulation, including VP's retention obligations under Article 29 of CSDR, VP shall delete data, including Ownership Information and personal data, received in connection with the Name Registration Services upon instruction from the Participant which has submitted the data. The procedure for deleting data is described in the User Guidelines.

5. Rights and obligations of the Participant

- 5.1. The Participant instructs VP through the Name Registration System in accordance with the procedures set out in the User Guidelines, to transmit (i) Ownership Information (except from CPR, CVR and other personal identification numbers) and (ii) the related Investor ID, to the Relevant Recipient for the

purpose of registering an investor in the ownership register of a security in scope of the Name Registration Services.

- 5.2. The Participant may only submit Ownership Information in respect of Securities Accounts maintained by the Participant in the VP system on behalf of its clients and in accordance with the requirements and procedures set out in the User Guidelines.
- 5.3. Subject to clause 5.4, when requesting a name registration or deregistration, the Participant shall provide VP with the following information:
 - (a) the relevant ISIN;
 - (b) information regarding the holding of securities to be name registered (which may be a subset of the total holding of a certain investor);
 - (c) the name and address of the investor;
 - (d) the effective date of the registration;
 - (e) the investor's CPR, CVR or other personal identification number, as applicable;
 - (f) the account number of the account held by the investor with the Participant and the corresponding account number of the omnibus account held by the Participant with VP; and
 - (g) any other information specified in the User Guidelines necessary for the provision of the Name Registration Services (collectively referred to as "Ownership Information").
- 5.4. The Participant shall submit Ownership Information to the Name Registration System no later than the cut-off time set out in the User Guidelines from time to time (the "Cut-Off Time") on each VP Business Day as specified on VP's website from time to time.
- 5.5. VP will on a best-efforts basis detect any duplicate registrations using Message ID, record date and initial date of shareholding. If any duplicates are detected, only the last incoming message will be forwarded to the Issuer or Relevant Recipient.
- 5.6. An investor may appoint another person to represent the investor in connection with name registration in an ownership register. Where such a representative has been appointed, the Participant shall provide information in accordance with clause 5.3 but only for the person who has been appointed to administer the management rights of the name registered shares. The User Guidelines further specify the provision of information specified in this Clause 5.6 and in Clause 5.3.
- 5.7. Where securities in respect of which a name registration has been requested are subsequently transferred or otherwise cease to be held by the relevant investor, the Participant shall instruct VP to forward a request to the Relevant Recipient for deletion or amendment of the relevant name registration in accordance with the procedures set out in the User Guidelines.
- 5.8. By submitting Ownership Information to VP in the Name Registration System in accordance with the procedures set out in the User Guidelines, the Participant shall be deemed to have instructed VP to (i) receive Ownership Information, and (ii) to transmit Ownership Information (except from CPR, CVR or other personal identification numbers) and the Investor ID to the Relevant Recipient for the purpose of effecting, amending or deleting a name registration of an

investor in the ownership register of a security in scope of the Name Registration Services.

- 5.9. The Participant represents and warrants that at the time any Ownership Information is submitted to VP:
- (a) the relevant investor (or third party in accordance with clause 5.6) is entitled to the rights attached to the securities concerned;
 - (b) the Ownership Information is complete, accurate and up to date representing the end of day status for the specified date; and
 - (c) the Participant is entitled to provide such Ownership Information and to instruct VP to process and transmit such Ownership Information for the purposes contemplated by these Name Registration Service Rules.
- 5.10. The Participant shall at all times be able to identify the underlying investor and shall be able to obtain sufficient records and documentation to substantiate the investor's name registration request of the relevant securities.
- 5.11. The Participant shall not submit Ownership Information to VP for the purposes of the Name Registration Services unless the Participant prior thereto has obtained all consents or established any other legal basis required under applicable law to enable VP to receive, retain, process and disclose such information in accordance with these Name Registration Service Rules. The Participant shall maintain and retain such consent or other legal basis, and evidence thereof, for as long as the relevant investor remains name registered.
- 5.12. The Participant shall provide VP with Ownership Information and any other information required for the Name Registration Services in a timely manner and in accordance with the operational deadlines, technical specifications and procedures set out in clauses 7 and 8 and in the User Guidelines.
- 5.13. The Participant bears sole responsibility for the validity and legitimacy of any request for registration, amendment or deletion of a name registration submitted through the Name Registration Services, including the accuracy, completeness or validity of the Ownership Information supplied to VP.
- 5.14. The Participant shall implement daily review procedures to verify data accuracy, completeness and validity and shall maintain copies of all submitted information.
- 5.15. The Participant shall provide instructions to VP regarding the deletion of CPR, CVR and other personal identification numbers in accordance with the procedure set out in the User Guidelines without undue delay once such data is no longer required for the purposes of the Name Registration Services.

6. Rights and obligations of Issuer

- 6.1. The Issuer is entitled to receive Ownership Information (except from CPR, CVR or other personal identification numbers) relating to those of its securities that are in scope for the Name Registration Services. Such information shall be made available by VP to the Relevant Recipient in accordance with clause 7.

- 6.2. The Issuer acknowledges and agrees that VP acts solely as an intermediary for the transmission of Ownership Information and that VP neither verifies nor guarantees the accuracy, completeness or validity of any Ownership Information received from a Participant.
- 6.3. The Issuer shall be the sole responsible for maintaining its ownership register in accordance with applicable law and for determining whether any person is entitled to be name registered therein.
- 6.4. The Issuer shall ensure that all information received through the Name Registration Services is used solely for lawful purposes and in accordance with applicable law, including applicable data protection legislation.
- 6.5. The Issuer shall notify VP without undue delay if the Issuer becomes aware of any error, omission, inconsistency or other matter affecting Ownership Information received by it through the Name Registration Services.
- 6.6. Where the Issuer has appointed another Relevant Recipient, the Issuer shall ensure that such Relevant Recipient complies with the requirements applicable to the Issuer under these Name Registration Service Rules. Any act or omission by the Relevant Recipient in connection with the Name Registration Services shall be deemed an act or omission of the Issuer.
- 7. Data and messages from VP**
- 7.1. Upon receipt of Ownership Information from the Participant, the Name Registration System performs various checks and technical validations as further described in the User Guidelines and provides an acceptance or rejection response. Note that the Name Registration System does not perform any reconciliation between the quantity of an ISIN reported by the Participant and the total quantity of an ISIN held in the relevant Securities Accounts in the VP system. The Participant is the sole responsible for detecting and correcting any discrepancy or error.
- 7.2. After Cut-Off Time on each VP Business Day, VP sends a status update message (as specified in the User Guidelines) to each Participant that has submitted updated Ownership Information in accordance with clause 8.1. on that VP Business Day.
- 7.3. After validation, cf. clause 7.1, and provided that such validation is successful, Ownership Information (except CPR, CVR or other personal identification numbers) received in the Name Registration System prior to Cut-Off Time on each VP Business Day will be segregated by ISIN and included in an end-of-day message batch (referred to as a "Business Day Message Batch") for the given VP Business Day in accordance with the procedure set out in the User Guidelines. Subsequently, the Ownership Information (except CPR, CVR or other personal identification numbers) segregated by ISIN is processed together with relevant Investor IDs and transmitted to the Relevant Recipient through the communication means, interfaces and procedures specified in the User Guidelines. Ownership Information received from Participants after Cut-Off Time will be included in the next Business Day Message Batch.

8. Data and messages from the Participant

8.1. The Participant shall send updated Ownership Information for securities in scope of the Name Registration Services in case of:

- changes in securities holding quantities;
- changes in securities account number held by the Investor with the Participant and/or the related Securities Account number maintained by the Participant with VP;
- closure or liquidation of investor accounts;
- changes to investor contact information;
- investors' wishing to be included or excluded from an ownership register;

and as further specified in the User Guidelines, no later than at Cut-Off Time each VP Business Day. Cut-Off Time and the seev message to be used for submitting the Ownership Information are specified in the User Guidelines.

8.2. The Participant is the sole responsible for the correctness and completeness of all instructions, information, etc. provided by it to VP. This includes that the Participant is responsible for correctly completing all relevant data fields, data boxes, etc. as further described in the User Guidelines.

9. Technical problems

9.1. The Name Registration Services are dependent on the availability and proper functioning of the Name Registration System, the VP system and certain third-party systems and infrastructure, including SWIFT. Maintenance activities, operational issues or other events affecting such systems or infrastructure may affect the availability or performance of the Name Registration Services and may result in delays in the generation, processing, receipt or transmission of Ownership Information, other data and messages.

9.2. Without prejudice to the liability provisions set out in Part 2 (General Terms and Conditions) of the VP Rule Book, VP shall not be liable for any delay, restriction or unavailability of the Name Registration Services resulting from maintenance activities, operational issues or other circumstances affecting the Name Registration System, the VP System or any other systems or infrastructure on which the Name Registration Services depend.

9.3. VP may postpone the Cut-Off Time if VP considers such postponement necessary or appropriate. Information regarding any revised Cut-Off Time shall be communicated to Participants and Relevant Recipients in accordance with the procedures set out in the User Guidelines. VP may also, with immediate effect and without prior notice, disconnect, suspend or otherwise restrict access to the Name Registration System if VP considers such action necessary or appropriate due to technical, operational, security or other circumstances, including in order to protect the integrity, availability or security of the VP System or the Name Registration System.

9.4. VP shall notify affected Participants and Relevant Recipients of any material interruption to the Name Registration Services in accordance with the procedures set out in the User Guidelines.

9.5. If a Participant or Issuer becomes aware of any error, defect, discrepancy or other issue affecting the Name Registration Services or any data, including Ownership Information, transmitted, received or processed in connection

therewith, the Participant or Issuer shall notify VP without undue delay and provide such information as VP may reasonably request.

- 9.6. If VP identifies, or is notified of, any error, omission, inconsistency or other defect in Ownership Information or other data received and/or transmitted through the Name Registration Services, VP may take such corrective measures as it reasonably considers necessary, including requesting the Participant to submit corrected or updated Ownership Information and transmitting corrected or updated Ownership Information to the Relevant Recipient.

10. Data Processing Agreement

- 10.1. By signing a Participation Agreement with VP which covers participation in the Name Registration Services the Participant and VP enter into the DPA outlined in Annex 1.

11. Fees

- 11.1. VP charges fees for the Name Registration Services provided to the Issuer and the Participant. All fees are charged in accordance with the terms contained in Part 2 (General Terms and Conditions) of VP Rule Book.
- 11.2. The Participant shall pay the fees applicable to the Name Registration Services as set out in the VP pricelist referred to in Part 2 (General Terms and Conditions) of VP Rule Book in force from time to time.
- 11.3. The Issuer shall pay the fees applicable to the Name Registration Services as set out in VP pricelist in force from time to time. The fees payable by the Issuer correspond to the fees payable in relation to the ownership register-related services provided by VP for segregated accounts in accordance with the established practice under Executive Order no. 819 of 26 June 2013.

12. Right to disclose

- 12.1. The Participant and the Issuer, respectively, authorise VP to disclose any relevant information related to the Name Registration Services to any governmental or other regulatory authority or court or other authority of competent jurisdiction, if such disclosure is required by law.

13. Liability rules

- 13.1. VP's liability for any delay, defect or error in connection with the provision of the Name Registration Services shall be governed by clause 5.6 of Part 2 (General Terms and Conditions) of VP Rule Book, with the adaptations which follow from these Name Registration Service Rules.
- 13.2. The Participant shall be liable for any loss, expense or claim, which is a result of incorrect or incomplete information, including Ownership Information, instruction, etc. provided by the Participant or a failure by the Participant to provide information, including Ownership Information, to the Name Registration System or VP in a timely manner.



- 13.3. VP is not liable for the accuracy, completeness or validity of any data, including Ownership Information, provided to the Issuer, or for any delay or failure by VP to receive, process or transmit the Ownership Information, unless caused by VP's wilful act or gross negligence.

14. Indemnification

- 14.1. The Participant shall hold harmless, reimburse, indemnify VP for losses arising from claims made by any third party related to the quality or timeliness of the Ownership Information, unless such loss was caused directly by VP's wilful act or negligence.

15. Termination rights

- 15.1. In addition to the terms concerning termination and breach contained in Part 2 (General Terms and Conditions) of the VP Rule Book, but subject to the rules contained in Part 4 (Settlement Rules) of the VP Rule Book on settlement in the event of Insolvency Proceedings, if any of the following events occur in respect of the Participant, VP has a right (but not an obligation) to suspend or terminate the Name Registration Services with immediate effect by giving notice to the Participant:
- (a) The Participant does not successfully perform such acts and tests as described in clause 3.8.
 - (b) A material or repeated breach under these Name Registration Service Rules is caused by the Participant, unless such breach is capable of being remedied and is remedied no later than 5 (five) VP Business Days after VP has given notice to the Participant in respect of the breach.
- 15.2. VP may terminate the provision of the Name Registration Services in general with 12 (twelve) months prior written notice to all Participants and Issuers participating in the Name Registration Services.
- 15.3. In addition to the terms concerning termination and breach contained in Part 2 (General Terms and Conditions) of the VP Rule Book, if any of the following events occur in respect of VP, the Participant or Issuer (as applicable) has a right (but not an obligation) to terminate its participation in the Name Registration Services with immediate effect by giving notice to VP:
- (a) A material or repeated breach under these Name Registration Service Rules is caused by VP, unless such breach is capable of being remedied and is remedied no later than 5 (five) VP Business Days after the Participant has given notice to VP in respect of the breach.
- 15.4. The Participant may terminate its participation in the Name Registration Services with 12 (twelve) months written notice to VP.

16. Automatic termination

- 16.1. The Name Registration Services delivered by VP to a Participant shall automatically terminate upon termination of the Participant's Participation Agreement.
- 16.2. The Name Registration Services delivered by VP to an Issuer shall automatically terminate upon termination of the Issuers' Issuance Agreement.

Annex 1 to VP Rule Book Part 7 (Name Registration Service Rules)

DATA PROCESSING AGREEMENT – NAME REGISTRATION SERVICES

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

(a) The Participant subscribing to the services in Part 7 (Name Registration Services) of VP Rule Book, whose identity, registration number, and contact details are set out in the Participation Agreement
(the data controller)

and

(b) VP Securities A/S, CVR no. 21599336, Nicolai Eigtveds Gade 8, 1402 Copenhagen, Denmark
(the data processor) or (Euronext Securities)

each a 'party'; together 'the parties'

HAVE AGREED on the following contractual clauses in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. PREAMBLE

1. These contractual clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.
2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 and repealing Directive 95/46/EC (General Data Protection Regulation).
3. In the context of the provision of the contract (hereinafter referred to as the Agreement), the data processor will process personal data on behalf of the data controller in accordance with the Clauses.
4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
5. Three appendices are attached to the Clauses and form an integral part of the Clauses.
6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
7. Appendix B contains a list of sub-processors authorised by the data controller.
8. Appendix C contains the minimum security measures to be implemented by the data processor.
9. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
10. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State¹ data protection provisions and the Clauses.
2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions are specified in Appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.
2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.
3. The data controller is obliged to reconsider the regulatory compliance of the instructions. The parties shall enter into dialogue regarding the instructions and the consequences which may arise from any potential unlawful instructions given by the data controller. The parties shall discuss amendments to the instructions given by the data controller to make it lawful and compliant with the Data Protecting regulation.

4. LIABILITY OF THE PARTIES

1. The liability for each party under this DPA shall be governed by the applicable limitations and exclusions of liability set out in the Agreement to which this DPA is appended.

5. CONFIDENTIALITY

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis.

¹ References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

6. SECURITY OF PROCESSING

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

- a. Pseudonymisation and encryption of personal data;
 - b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.
 - c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
 - d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.
 3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify in writing, including by electronic means, these additional measures to be implemented in Appendix C.

7. USE OF SUB-PROCESSORS

1. On the commencement of the Clauses, the data controller shall authorise the use of sub-processors for the processing described for that party. The list of sub-processors already authorised by the data controller can be found in Appendix B.1.
2. The data processor can, during the course of this DPA, decide to choose and engage another processor (sub-processor) to carry out specific processing activities on behalf of the data controller.
3. To engage and choose another processor (sub-processor), the data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor). The data processor must ensure that the sub-processor complies with GDPR and contractual obligations, including appropriate technical and organizational measures.



The data processor shall inform in writing the data controller one (1) month in advance about any intended changes concerning the addition or replacement of sub-processors and any changes in the processing agreed on.

4. The data controller may object to the use of a sub-processor. To exercise this right, the data controller must provide written notice to the data processor within thirty (30) days of receiving the notification of change from the data processor. The objection must be relevant and based on data protection related considerations.

In the event that the objection submitted by the data controller meets the above requirements, the data processor must take the objection into account. If the data processor is unable to meet the objection of the data controller, the data controller is entitled with one (1) month's written notice to terminate the part of the agreement that includes the specific service for which the sub-data processor otherwise would have access to personal data. The remaining part of the agreement will remain in force in accordance with the provisions of the agreement.

8. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

1. Any transfer of personal data to third countries or international organisations by the data processor or instructed by the data controller on the basis of documented instructions from the data controller shall always take place in compliance with Chapter V GDPR.
2. In the absence of documented instructions from the data controller, the data processor shall nonetheless be authorised:
 - to transfer personal data, provided such transfer is in compliance with Chapter V of the GDPR.
 - to transfer to third countries or international organisations, where such transfer is required under EU or Member State law to which the data processor is subject.
3. The data controller reserves the right to object to such transfers performed by the data processor, with any objections to be made in accordance with Clause 7.4.

9. ASSISTANCE TO THE DATA CONTROLLER

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

- a. the right to be informed when collecting personal data from the data subject
- b. the right to be informed when personal data have not been obtained from the data subject
- c. the right of access by the data subject
- d. the right to rectification
- e. the right to erasure ('the right to be forgotten')
- f. the right to restriction of processing
- g. notification obligation regarding rectification or erasure of personal data or restriction of processing
- h. the right to data portability
- i. the right to object
- j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:
 - a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
 - b. The data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
 - c. The data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
 - d. The data controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.
3. The data processor must assist the data controller with meeting the other obligations that may be incumbent on the data controller according to Union or member state law where the assistance of the data processor is implied, and where the assistance of the data processor is necessary for the data controller to comply with its obligations.

10. NOTIFICATION OF PERSONAL DATA BREACH

1. In case of any personal data breach, the data processor shall without undue delay after having become aware of it, notify the data controller of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.
2. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:
 - a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
 - b. The likely consequences of the personal data breach;
 - c. The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
3. The elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority shall as far as possibly cover the elements below:
 - a. A description of the incident including the physical location for the incident;
 - b. A list of sequences of the incident including information about when the incident began, the findings and (expected) closing time;
 - c. The nature of the breach of personal data security, including any technology involved, the categories of information and data subjects and the approximate number of data subjects affected and, if possible, the approximate number of records;
 - d. A general assessment of the probable consequences for the data subjects;

- e. A description of the measures the data processor has taken or/and proposed to the data controller to handle the incident and to reduce the impact of the personal data breach;
- f. Final or if and how further information shall follow;
- g. Information about from who the data controller can get more information if needed.

11. ERASURE AND RETURN OF DATA

1. On termination of the provision of personal data processing services, the data processor shall be under the obligation to either delete or return the personal data to the data controller on the data controller's request. In the event of returning the personal data, the data processor shall delete existing copies unless Union or Member State law requires storage of the personal data.
2. The data controller can, after the signature of the contract, modify the data controller's original choice regarding the erasure and return of the personal data. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

12. AUDIT AND INSPECTION

1. Compliance with the obligations laid down in Article 28 and the Clauses allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller. The auditor mandated to conduct the audits and inspections shall not be a competitor of the data processor.
2. The data controller shall have the right to request at the data controller's expense and no more than once per calendar year:
 - the data processor to provide for the necessary information to demonstrate the data processor's compliance with this Agreement,
 - request an audit or inspection under the following circumstances:
 - where required by a competent authority under applicable Personal Data Processing Legislation; or
 - in connection with a confirmed Personal Data breach.
3. The data processor shall allow for and contribute to audits conducted by the data controller, or an auditor mandated by the data controller, provided that such auditor is not a direct competitor of the data processor.
4. Assistance by the data processor in facilitating the audit shall be subject to prior agreement between the Parties regarding the scope, timing, and duration of the audit, and shall require the data controller's prior written approval of any costs incurred by the data processor in providing such assistance.
5. The data processor shall immediately inform the data controller if, in its opinion, any request or instruction related to the audit infringes applicable Personal Data Processing Legislation or other relevant data protection provisions under Union or Member State law.
6. In case data controller wants to audit the data processor, the data controller shall:
 - inform the data processor by prior written notice of thirty (30) calendar days;
 - observe all of the data processor's security policies, procedures and measures in place at the time of such audit and, in case the audit takes place at the data processor's premises, conduct such audit:
 - strictly within the limits of the policies, procedures and measures regarding access to and use of data processor's facilities taken into account the regulatory status of this latter;
 - in the presence of the data processor's staff members, advisors or contractors designated by the data

- processor for this purpose;
- during normal business hours and minimize disruption to the data processor's operations;
 - limit the audit to Personal Data Processing activities and shall not include general business operations, financial records, or unrelated data;
 - conduct the audit within a mutually agreed timeframe to minimize disruption to the data processor's business operations and ensure minimal interference with its activities;
 - keep all information relating to data processor (such as, but not limited to the Processor's products and services, operations, customers, members, prospects, know-how, design rights, trade secrets, market information and/or business affairs, etc.) obtained during an audit confidential ("Confidential Information"), unless if it concerns public information;
 - not use the Confidential Information for any purpose other than to carry out the audit;
 - not disclose Confidential Information to any third party save to its employees, officers and agents to the extent necessary in the framework of such audit and provided that the data controller ensures that such employees, officers and agents are aware of and comply with the confidentiality terms of this article;
 - not copy, in whatever way or form, Confidential Information, unless such information is necessary for the audit and return, delete and destroy (in primary and backup) all Confidential Information after termination of the audit;
 - notify the data processor immediately and provide relevant details if any non-compliance is discovered during an audit.
7. The data processor may object to an audit if:
- it is not conducted in accordance with the agreed scope, notice period, or confidentiality obligations;
 - it interferes excessively with the data processor's business operations;
 - the data controller fails to justify the necessity of the audit under data protection laws.
8. The data controller shall:
- not use any audit findings to gain a competitive advantage over the data processor,
 - ensure that audit reports remain strictly confidential and are not disclosed to third parties, regulatory authorities, or any competitors of the data processor unless legally required.

13. THE PARTIES' AGREEMENT ON OTHER TERMS

The parties may agree other clauses concerning the provision of the personal data processing service specifying, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. COMMENCEMENT AND TERMINATION

1. The Clauses shall become effective on the date of both parties' signature.
2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.
3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless

other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11, the Clauses may be terminated by written notice by either party.

15. DATA CONTROLLER AND DATA PROCESSOR CONTACTS/CONTACT POINTS

1. The parties may contact each other using the following contacts/contact points:

Data controller:

Name: *The data controller is the Participant as defined in the VP Rulebook, whose identity, registration number, and contact details are set out in the applicable Participation Agreement.*

Data processor:

For notification in relation to the provision of the service:

Name Nordic Client Services
E-mail CPH-Clientsupport@euronext.com

For notification in relation to GDPR requests:

Name Celine Debest
Position Head of Corporate Compliance - Data Protection Officer
Email dpo@euronext.com

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

APPENDIX A - INFORMATION ABOUT THE PROCESSING

A.1. Description of the purposes and ways of Processing Personal data (please, also include a detailed description of the procedural workflow):

Purpose of the Processing	Name Registration Services as described in Part 7 (Name Registration Service Rules) of 7 VP Rule Book
Categories of Personal data	The Name Registration Services collects and processes the following categories of personal data provided by CSD participants in relation to registered investors for each ISIN: • Identity details, including name, address, and identification numbers (such as CPR, CVR, or LEI) • Contact information, including home address, business address, and email address • Third party information, where relevant, such as details of authorised representatives or legal guardians • Account numbers and name registered holdings

	The personal data is collected for the purpose of maintaining the Share Register each ISIN, enabling daily updates and, where required, full data loads at the request of the Issuer.
Categories of Data subject	The personal data processed by the Name Registration service relates to the following data subjects: • Name registered investors who hold securities identified by an ISIN in the omnibus accounts of CSD participants • Authorised representatives or legal guardians of name registered investors, where applicable The processing of personal data is limited to these data subjects and is conducted solely for the purpose of maintaining the Share Register each ISIN, as described in this agreement.

A.2. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The data processing is not limited in time and shall last for as long time as the data processing is relevant for the data processor's performance of the agreed task and in compliance with obligations to the data controller stated in the Agreement.

APPENDIX B - AUTHORISED SUB-PROCESSORS

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	COMPANY REGISTER NUMBER	ADDRESS	HOSTING LOCATION	DESCRIPTION OF PROCESSING
Euronext Technologies SAS	425 100 294	14 Place des Reflets 92400, Courbevoie, France	14 Place des Reflets 92400, Courbevoie, France	Cyber security awareness. End-user support
Euronext Technologies Unipessoal LDA	513945342	Avenida da Boavista, 3433 4100-138 Porto Portugal	Avenida da Boavista, 3433 4100-138 Porto Portugal	Cyber security awareness. End-user support

APPENDIX C - INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

C.1. Security of processing

The level of security shall take into account:

Taking into account the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or alteration to personal data and the nature of personal data to be protected, the data processor shall take all the measures that are required in accordance with Article 32 of the Data Protection regulation to safeguard the personal data from unauthorized disclosure or access and against all other unlawful forms of processing the data processor has implemented technical and organizational security measures. The data controller agrees that these measures ensure an appropriate level of security, taking into account the nature of

the processing, the state of technology and the costs of their implementation. The data processor shall be entitled to modify those measures, provided that it informs the data controller and ensures that the modified measures offer at least equivalent security to the personal data.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Information Security Policy

The data processor shall produce and maintain an information security policy which have been approved by the management of the data processor and which, as a minimum, describes:

- a) The management's overall guidelines for information security;
- b) A requirement for the support and commitment to comply with all relevant legislative requirements on data protection and the agreed requirements from the data controller;
- c) Rules and guidelines for determining an acceptable level of risk.

Encryption of personal data

In consideration of legal requirements, requirements from the data controller risks and pertinence the data processor shall make use of pseudonymisation and/or relevant encryption technologies and other similar measures.

Ongoing confidentiality, integrity, availability and robustness of systems and services

Based on the classification of data, the data processor introduces multilayer protection of systems and data to ensure confidentiality, integrity, availability and robustness of the processing systems. Only authorized persons shall have access to the personal data which are being processed. It is only persons who are engaged in the purposes for the processing of the personal data, can be authorized. The users cannot be authorized to use or processing which are not needed. In addition persons for whom access to data is necessary in order to perform audit, revision, operational or system technical tasks, can also be authorized. The data processor shall implement measures to secure that only authorized users can have access, and that these users will only have access.

The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Based on the requirements from the data controller, the data processor introduces processes and systems to ensure timely recovery of and access to the personal data in the event of a physical or technical incident.

Procedures for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

The data controller maintains procedures for regularly testing, assessment and evaluation of the effectiveness of the measures for these testings. Testings are performed on a regular basis.

Requirements for access to data online

N/A.

Requirements for the protection of data during transmission

The data processor introduces appropriate protection of personal data during transmission, e.g. by encryption, in proportion to the classification of data.

Requirements for the protection of data during storage

The data processor introduces appropriate protection of personal data during storage, e.g. by encryption or access management, in proportion to the classification of data.

Requirements for physical security of locations at which personal data are processed.

The data processor shall ensure appropriate physical security of locations at which personal data are processed. The physical access to locations where the personal data is processed, shall be secured against unauthorized persons' access to that data. As an example, this can entail locking of the relevant facilities, use of admittance cards, alarm systems and watchmen, and specific restrictions to the access to server rooms.

Education/instructions

Employees of the user administration shall have the necessary education/instruction to secure compliance with these rules.

Requirements for the use of home/remote working

Personal data must only be processed in or from approved facilities or by approved and secured remote access. The data processor does not offer permanent home offices or remote workstations.

Logging

The data processor must be able to generate overviews of users and assigned rights as well as groups and roles, including the users' use of accounts, particularly for the purpose of control and follow-up. The overview shall document the grouping of rights, added, altered or deleted rights and the appertaining time stamps. The overview shall be delivered to the data controller upon request.

For the purpose of the handling of incidents the data processor shall ensure logging of major incidents.

Special requirements to security measures that apply to the data controller

N/A.