Nasdaq Global Data Agreement
Data Processing Addendum
Controller to Controller

I. Application

Distributor has entered the Nasdaq Global Data Agreement with Nasdaq, Inc., pursuant to which Nasdaq provides certain Information and Services to Distributor (the "**Service**"). For the purpose of this Data Processing Addendum (the "**DPA**") Nasdaq, Inc. and/or its affiliates or subsidiaries shall be collectively referred to as "**Nasdaq**" and Distributor and/or its affiliates or subsidiaries shall be collectively referred to as "**Distributor**".

Under the Agreement Nasdaq and Distributor may process Personal Data (as defined below). To the extent any Distributor entity inside the EEA, UK or Switzerland (collectively, "**Europe**"), in connection with fulfilling the Agreement, transfers Personal Data to Nasdaq outside of Europe for the purpose of Nasdaq processing such Personal Data for its own purposes (i.e. Nasdaq being a *data controller*) the provisions of this DPA shall apply to such processing. Nasdaq entities outside of Europe shall be deemed "*data importers*" and Distributor entities shall be deemed "*data exporters*" for this DPA. The parties specifically note that this DPA shall only apply to processing of Personal Data when such Personal Data is transferred from Distributor inside Europe as a *data controller* to Nasdaq outside of Europe as a *data controller* and specifically shall not apply to the situations where Personal Data is processed by the Distributor as *data processor* or situations where any transfer of Personal Data between the parties is maintained within Europe. For the purpose of the foregoing *data controller* and *data processor* shall be deemed to have the meaning given to them in the GDPR, UK GDPR, or Swiss FDAP (or any superseding legislation), as applicable.

This DPA, last updated on November 6, 2024, is subject to the terms of, and fully incorporated and made part of, the Agreement. This DPA shall amend and supplement any provisions relating to the processing of Personal Data contained in the Agreement, and shall be effective for the term of the Agreement unless terminated earlier as set out below.

II. Definitions

For the purposes of this DPA, the following terms shall have the following meanings:

"EEA" means the European Economic Area.

"Data Subject", "Personal Data" and "Processing" means as defined in the GDPR, UK GDPR, or Swiss FADP, as applicable.

"Swiss FADP" means the Swiss Federal Act on Data Protection 2020, including its implementing ordinances.

"GDPR" means 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 (General Data Protection Regulation).

"Standard Contractual Clauses" means the Commission Implementing Decision (EU) 2021/914 establishing Standard Contractual Clauses for data transfers to Third Countries (as amended, modified, or replaced from time to time); specifically, the applicable module within the Standard Contractual Clauses is MODULE ONE (Transfer Controller to Controller), as may be updated or replaced by the European Commission from time to time. For the avoidance of doubt, MODULE TWO (Transfer Controller to Processor), MODULE THREE (Transfer Processor to Processor), and MODULE FOUR (Transfer Processor to Controller) do not apply to this DPA.

"Third Country" means a country outside the European Union, the EEA, the UK, or Switzerland.

"UK GDPR" means the United Kingdom (UK) General Data Protection Regulation.

"UK International Data Transfer Addendum" means the International Data Transfer Addendum to the Standard Contractual Clauses version B1.0, in force 21 March 2022 as adopted under the UK GDPR or such successor clauses as may be adopted by the UK.

All other capitalized terms not defined herein shall have the meaning set forth in the Agreement.

III. Additional Terms:

A. In order to enable Distributor to meet cross-border transfer requirements under applicable data protection laws in Europe, the parties hereby agree that the terms of the Standard Contractual Clauses shall apply, including the appendices attached thereto, where Personal Data is transferred from the Distributor as a controller located in Europe to Nasdaq as a controller, where Nasdaq receives such Personal Data in a Third Country, and that the terms of the Standard Contractual Clauses shall supersede any conflicting terms in the Agreement and this DPA. The parties further agree that the Standard Contractual Clauses are incorporated by reference into this DPA, and the remaining details required under the Standard Contractual Clauses are deemed completed, as appropriate, with the information set forth in this DPA, including the appendices to this DPA. For purposes of the Standard Contractual Clauses, the parties agree:

a) The Personal Data Processing activities in Appendix 1 to the Standard Contractual Clauses will be such activities as described in the Agreement; the categories of Data Subjects and categories of Personal Data in Appendix 1 to the Standard Contractual Clauses will be those provided by Distributor to Nasdaq pursuant to the Agreement as set forth in Appendix 1 (Processing Details) to this DPA; and the data security measures in Appendix 2 to the Standard Contractual Clauses will be those identified in Appendix 2 (Information Security Program) of this DPA.

b) The optional language in Clause 11 (Redress) shall not apply;

c) For Clause 13 (Supervision), the Supervisory Authority with responsibility for ensuring compliance by the data exporter with the GDPR with regard to such transfers, namely, the lead Supervisory Authority of the exporting Distributor entity, shall act as the competent Supervisory Authority;

d) For Clause 17 (Governing Law), Option 2 shall apply and that, in the event that the law of the jurisdiction in which the data exporter is established does not allow for third-party beneficiary rights, the Standard Contractual Clauses shall be governed by the laws of Sweden; and

e) For Clause 18 (Governing Law), the parties agree that courts of the jurisdiction in which the data exporter is established shall resolve any dispute arising from the Standard Contractual Clauses.

B. Transfers Under UK GDPR. To the extent that Distributor transfers Personal Data that is subject to the UK GDPR cross-border data transfer restrictions to Nasdaq in a Third Country, the parties agree that the UK International Data Transfer Addendum to the Standard Contractual Clauses will also apply to such transfer, which are incorporated by reference into this DPA, and the remaining details required under the UK International Data Transfer Addendum are deemed completed, as appropriate, with the information set forth in this DPA, including the appendices to this DPA. The categories of Data Subjects, purposes of transfer(s), recipients, and categories of Personal Data in Annex B to the UK International Data Transfer Addendum will be as set forth in Appendix 1 (Processing Details) to this DPA. In the event of any inconsistency between the terms of the UK International Data Transfer Addendum and any terms of this DPA with respect to such transfers subject to the UK GDPR, the terms of the UK International Data Transfer Addendum will govern and control with respect to such transfers.

C. Transfers Under Swiss FADP. To the extent that Distributor transfers Personal Data that is subject to the Swiss FADP cross-border data transfer restrictions to Nasdaq in a Third Country, the parties agree that the Standard Contractual Clauses with the details as set out in Section III.A above and amended as follows will apply to such transfers to the extent required by the Swiss FADP:

a) References to the GDPR in the Standard Contractual Clauses are to be understood as references to the FADP insofar as the transfer is subject exclusively to the FADP and not to the GDPR;

b) The term “member state” in the Standard Contractual Clauses shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses.

c) For Clause 13 (Supervision), the following subsections 3.5.3.1 and 3.5.3.2 will apply and are hereby deemed added to Section 3.1 of Appendix 1 (Processing Details) of this DPA:

- Where the transfer is subject exclusively to the Swiss FADP and not the GDPR, the Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner;
- Where the transfer is subject to both the Swiss FADP and the GDPR, the Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the Supervisory Authority is as set forth in Section 3.1 d) above insofar as the transfer is governed by the GDPR.

D. To the extent this DPA applies to Personal Data transferred by Distributor to Nasdaq, Nasdaq assumes all rights and obligations as “data importer” of such Personal Data under the Standard Contractual Clauses and Distributor assumes all rights and obligations as “data exporter” under the Standard Contractual Clauses of such Personal Data.

E. Nasdaq may terminate the Standard Contractual Clauses or UK International Data Transfer Addendum (i) if and when the Agreement expires or is terminated or (ii) if Nasdaq offers an alternative compliance standard for the lawful transfer of Personal Data to the Third Country in which Nasdaq receives the Personal Data recognized under applicable law. Distributor may terminate the Standard Contractual Clauses or UK International Data Transfer Addendum at Distributor’s discretion by written notice pursuant to the notice terms provided in the Agreement.

F. The Agreement and Sections A through H of this DPA shall apply only between the parties and shall not confer any rights to any third parties. With respect to the rights and obligations of the parties vis-à-vis each other, and if and to the extent either party asserts rights or remedies against the other party, the terms of this DPA shall control.

G. Distributor represents and warrants that it has complied with applicable law, including data protection laws, related to its collection, processing and transfer of Personal Data to Nasdaq and further represents and warrants that, to the extent required by applicable law, it has obtained all necessary consents from and/or provided all necessary notices to data subjects for Nasdaq to use such Personal Data that it receives as a controller from Distributor for its own lawful business purposes. Except as expressly stated otherwise, in the event of any conflict between the terms of the Agreement and the terms of this DPA, the relevant terms of this DPA shall take precedence.

H. All other terms and conditions of the Agreement remain unchanged.

APPENDIX 1

Processing Details

1. LIST OF PARTIES

DATA EXPORTER(S)	
Name	Distributor and/or its affiliates or subsidiaries
Address	The address for Distributor as set forth in the Agreement
Contact person's name, position and contact details	The contact details for Distributor as set forth in the Agreement
Activities relevant to the data transferred under the Standard Contractual Clauses	Provision of reporting and license data pursuant to the Agreement
Signature and date	Distributor's signature and date on the Agreement
Role (controller/processor)	Data Controller

DATA IMPORTER(S)	
Name	Nasdaq and its affiliates or subsidiaries
Address	The address for Nasdaq as set forth in the Agreement
Contact person's name, position and contact details	The contact details for Nasdaq as set forth in the Agreement
Activities relevant to the data transferred under the Standard Contractual Clauses	Receipt of the Personal Data pursuant to the Agreement
Signature and date	Nasdaq's signature and date on the Agreement
Role (controller/processor)	Data Controller

2. DESCRIPTION OF THE TRANSFER

2.1 Categories of data subjects whose personal data is transferred

End users of data (or their designees or representatives) of information flows originating and/or distributed by Nasdaq (either directly to the end user or through a distributor to an end user).

2.2 Categories of personal data transferred

For external Subscribers: Name, Employer, Occupation, Employer Address, Employment Status, Email Address, entitlements Information, Start and end dates related to the access or provisioning of information, records relating to actual usage of Information.

For Internal Subscribers: Name, User Id, Occupation/Role, entitlements Information, Other Information used to identify internal subscribers access to Information, start and end dates related to the access or provisioning of Information, records relating to actual usage of Information.

2.3 Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- N/A

2.4 The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Periodic

2.5 Nature of the processing

To fulfill reporting obligations, ensure compliance with, and exercise audit, review and other rights pursuant to, the terms and conditions of the Global Data Agreement

2.6 Purpose(s) of the data transfer and further processing

To fulfill reporting obligations, ensure compliance with, and exercise audit, review and other rights pursuant to, the terms and conditions of the Global Data Agreement

2.7 The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As long as necessary for the purposes identified above or as otherwise required for compliance with Nasdaq policies and applicable law.

2.8 For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- N/A

3. COMPETENT SUPERVISORY AUTHORITY

- As provided in Section III.A.c of this DPA.

APPENDIX 2

Information Security Program

Taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons. Nasdaq has implemented, and will maintain, a comprehensive written information security program ("**Information Security Program**") with respect to the Personal Data transferred to or received by Nasdaq pursuant to the Agreement that includes administrative, technical, and physical safeguards to ensure the confidentiality, security, integrity, and availability of Personal Data and to protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data.

In particular, the Information Security Program will include the following safeguards where appropriate or necessary to ensure the protection of Personal Data:

Measures of pseudonymisation and encryption of personal data

- Access Controls – policies, procedures, and physical and technical controls to encrypt and decrypt Personal Data where appropriate.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- Information Security Program – a comprehensive written information security program that includes administrative, technical, and physical safeguards to ensure the confidentiality, security, integrity, and availability of Personal Data and to protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data.
- Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Personal Data or systems that contain Personal Data, including a data backup plan and a disaster recovery plan.

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

- Security Incident Procedures – policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Personal Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.
- Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Personal Data or systems that contain Personal Data, including a data backup plan and a disaster recovery plan.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- Testing – The data importer will regularly test the key controls, systems and procedures of its Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

Measures for user identification and authorization

- Access Controls – policies, procedures, and physical and technical controls: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons; (ii) to ensure that all members of its workforce who require access to Personal Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access; and (iii) to authenticate and permit access only to authorized individuals and to prevent members of its workforce from providing Personal Data or information relating thereto to unauthorized individuals.

- Data Integrity – policies and procedures to ensure the confidentiality, integrity, and availability of Personal Data and protect it from disclosure, improper alteration, or destruction.

Measures for the protection of data during transmission

- Storage and Transmission Security – technical security measures to guard against unauthorized access to Personal Data that is being transmitted over an electronic communications network, including a mechanism to encrypt Personal Data in electronic form while in transit and in storage on networks or systems to which unauthorized individuals may have access.

Measures for the protection of data during storage

- Storage Media – policies and procedures to ensure that prior to any storage media containing Personal Data being assigned, allocated or reallocated to another user, or prior to such storage media being permanently removed from a facility, the data importer will delete such Personal Data from both a physical and logical perspective, such that the media contains no residual data, or if necessary physically destroy such storage media. The data importer will maintain an auditable program implementing the disposal and destruction requirements set forth in this section for all storage media containing Personal Data.

Measures for ensuring physical security of locations at which personal data are

Processed

- Information Security Program – a comprehensive written information security program that includes administrative, technical, and physical safeguards to ensure the confidentiality, security, integrity, and availability of Personal Data and to protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data

Measures for ensuring events logging

- Audit Controls – hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith.

Measures for ensuring system configuration, including default configuration

- Audit Controls – hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith.

Measures for internal IT and IT security governance and management

- Assigned Security Responsibility – The data importer will designate a security official responsible for the development, implementation, and maintenance of its Information Security Program. The data importer will inform the data exporter as to the person responsible for security.
- Adjust the Program – The data importer will monitor, evaluate, and adjust, as appropriate, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of the Personal Data, internal or external threats to the data importer or the Personal Data, and the data importer's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems. In light of the foregoing, the Information Security Program is subject to change; provided, however, that any such update will not lessen the applicable information security protections.

Measures for certification/assurance of processes and products

- Testing – The data importer will regularly test the key controls, systems and procedures of its Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

- Adjust the Program – The data importer will monitor, evaluate, and adjust, as appropriate, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of the Personal Data, internal or external threats to the data importer or the Personal Data, and the data importer's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems. In light of the foregoing, the Information Security Program is subject to change; provided, however, that any such update will not lessen the applicable information security protections.

Measures for ensuring data quality

- Data Integrity – policies and procedures to ensure the confidentiality, integrity, and availability of Personal Data and protect it from disclosure, improper alteration, or destruction.

Measures for ensuring limited data retention

- Device and Media Controls – policies and procedures on hardware and electronic media that contain Personal Data into and out of a data importer facility, and the movement of these items within a data importer facility, including policies and procedures to address the final disposition of Personal Data, and/or the hardware or electronic media on which it is stored, and procedures for removal of Personal Data from electronic media before the media are made available for re-use.
- Storage Media – policies and procedures to ensure that prior to any storage media containing Personal Data being assigned, allocated or reallocated to another user, or prior to such storage media being permanently removed from a facility, the data importer will delete such Personal Data from both a physical and logical perspective, such that the media contains no residual data, or if necessary physically destroy such storage media. The data importer will maintain an auditable program implementing the disposal and destruction requirements set forth in this section for all storage media containing Personal Data.

Measures for ensuring accountability

- Security Awareness and Training – a security awareness and training program for all members of the data importer's workforce (including management), which includes training on how to implement and comply with its Information Security Program
- Audit Controls – hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith.

Measures for allowing data portability and ensuring erasure

- Device and Media Controls – policies and procedures on hardware and electronic media that contain Personal Data into and out of a data importer facility, and the movement of these items within a data importer facility, including policies and procedures to address the final disposition of Personal Data, and/or the hardware or electronic media on which it is stored, and procedures for removal of Personal Data from electronic media before the media are made available for re-use.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Nasdaq shall ensure Processors provide technical and organizational measures no less protective than those set forth in the DPA, including this Appendix 2 (Information Security Program).