

# Information Protection and Privacy Practices

As a global technology company and exchange operator, Nasdaq views data as its lifeblood. Accordingly, we are committed to appropriately securing non-public data used as part of our business operations, including information that Nasdaq generates in the performance of its services, and data provided to us by third parties, including customers, vendors, business partners, employees and other stakeholders.

### OUR VISION

Reimagining markets to realize the potential of tomorrow.

### OUR MISSION

We bring together ingenuity, integrity, and insights to deliver markets that accelerate economic progress and empower people to achieve their greatest ambitions.

### OUR VALUES:

- We put **Clients First**
- We act with **Integrity**
- We are **Passionate**
- We lead **Innovation**
- We are **Effective**
- We are **Resilient**

This commitment is reflected in our engrained culture of security, our robust policies and procedures for data systems and processing activities, our mechanisms for monitoring our information systems and data use, the role-based training that we provide to staff on data protection, and the team of skilled information security and technology professionals who design, protect, and maintain our information systems. Reflecting the unique risks and potential harm posed by mishandling or misuse of personal data, Nasdaq's privacy program builds on the foundation of our information security program to apply special governance, policies, procedures and training on the use, handling and processing of personal data and performance of activities that impact privacy rights (as determined by the jurisdictions in which we operate).

## Nasdaq Guiding Principles – Information Protection

As set forth in the Nasdaq Code of Ethics, Nasdaq personnel are expected to protect and secure the confidentiality of non-public information that they receive, access or create in connection with their work at the company. This includes adhering to any laws, regulations and/or non-disclosure agreements that restrict the use of data, require measures to safeguard it, and limit disclosure of information. It also requires that personnel limit their use of information technology assets (e.g., laptops, phones and other devices) to permitted activities so that data is not put at risk, and that they promptly report any suspected improper use or potential disclosure of data.

To support these principles, Nasdaq maintains a comprehensive and consistent set of information security documentation and requirements intended to ensure the security, reliability, integrity, accuracy, confidentiality, and availability of Nasdaq information assets. These documents record the security controls and personnel responsibilities established to protect Nasdaq information and information systems against both accidental and unauthorized access, modification, interference, disclosure, and destruction. These include our Information Security Policies, which apply to personnel (both employees and contractors) working for Nasdaq. Our Information Security Policies establish the following primary requirements:

- Nasdaq information and systems should be protected in a manner commensurate with their sensitivity, value and criticality; protections for information and systems should be maintained in due proportion with applicable and emerging threats.
- Nasdaq information and systems should be used only in an approved, ethical, and lawful manner.
- Nasdaq data should be classified using our internal data classification schema to ensure consistent handling and protection.

Nasdaq Information Security Policies are further supported by detailed Information Security Standards, Information Security Guidelines, and Security Technical Implementation Guides, which each provide greater detailed requirements for specific systems and information technology activities.

## Nasdaq Guiding Principles – Personal Data and Privacy

Nasdaq recognizes that special obligations may attach to situations where it receives or processes personal data as part of its operations. This can extend to data supplied by personnel in connection with their employment or contracted work with Nasdaq, information provided by clients to support their work with Nasdaq or deliver contracted services, or members of the public who wish to receive information or materials that we generate or use publicly available services that we offer.

As set forth in our Code of Ethics, Nasdaq is committed to respecting and complying with laws and regulations that apply to the collection, use, distribution, destruction, and other processing of personal data. Subject to local legal requirements, personal data encompasses any data about an identified or identifiable individual.

In following the requirement of the Code of Ethics, we expect employees to handle personal data using the “minimum necessary” standard. This means that employees

should use such data only as permitted and necessary to our work and disclose such information only to authorized recipients for them to perform their work. In particular:

- Where information is gathered from one of our public websites, employees should adhere to the privacy policy in effect for the site at the time it was collected,
- Employees should comply with contract requirements with customers, suppliers, and others related to processing personal data,
- Employees should adhere to the Global Employee Privacy Policy and European Union Employee Privacy Policy (as applicable) when handling employee data.

When using and storing personal data, employees should secure it in compliance with the Data Classification Policy and other relevant Information Security Policies and Standards as well as contractual requirements.

Nasdaq respects individuals’ ability to exercise their legal rights over their personal data, including, as allowed under applicable law, the right to obtain and correct information and the right to have information deleted. Any questions related to our Privacy Program should be directed to [privacy@nasdaq.com](mailto:privacy@nasdaq.com).

## Engagement in Information Protection and Privacy Community

Nasdaq is committed to being an active participant in relevant industry groups and forums related to information security and privacy, so that our programs can stay abreast of risks, industry practices, and emerging trends. We also seek to contribute thought leadership in these areas through active engagement.

We will periodically review this *Information Protection and Privacy Practices Statement* to reflect our current activities.

---

This statement reflects Nasdaq’s expectations and aspirational standards for its own business. Specific current requirements for conduct are found within relevant provisions the operative Nasdaq Code of Ethics, Employee Handbooks and company policies. The inclusion of a statement in this document does not constitute a representation regarding past or future performance. This statement relates only to Nasdaq’s internal business operations only; Nasdaq recognizes that one-size does not fit all and that different standards are appropriate for different companies. Expectations and requirements for Nasdaq listed companies, exchange members and other market participants are found in the applicable rulebooks, published standards and applicable laws and regulations.