Our Approach to Data & Information Security

March 2022

About this Statement

This statement is designed to outline Morningstar's approach to data and information security.
For more information on related policies, please visit Morningstar's Sustainability Policies & Reports Center, the Privacy Center, or the Investor Relations site.

Our Approach

Morningstar maintains comprehensive information security and privacy programs designed to manage the security and privacy of customers' personal data. The information security program includes comprehensive vulnerability assessment capabilities which cover servers, employee workstations, as well as cloud environments. The security of cloud infrastructure is implemented in a multi-layered manner, achieved through cloud security standards, and accounts are actively scanned for configuration drift.

How do we define vulnerability?

We follow the definitions of vulnerability and data security risk as defined in the SASB (Sustainability Accounting Standards Board) Standards.

- **Vulnerability** is defined as a weakness in an information system, system security procedures, internal controls, and/or implementation that could be exploited.

Vulnerabilities in Morningstar's systems are proactively addressed by a regular patching schedule for servers and workstations. All vulnerabilities are further governed by industry-standard remediation service levels and tracked in a ticketing system which also provides a high-level risk view. Our threat intelligence team monitors trends in the threat landscapes and works with our internal stakeholders to address critical threats in a timely manner.

For all in-house developed software, Morningstar follows a secure software development lifecycle which incorporates architecture reviews, change management, and code scans a well as dynamic testing of our products in dedicated test environments. Furthermore, we use third-party testing providers to perform penetration tests of critical applications and annually of our Internet-facing network perimeter.

Our Principles

We require that our team follow the following principles when processing personal data:

- Processing must be lawful and fair. We will only process personal data in accordance with applicable privacy laws.
- We're transparent about how we use personal data. We notify data subjects about how we collect their data, how we use it, and how we share it.
- We only use personal data for the purpose for which it was collected or with customers' consent.
- We give our customers meaningful opportunities to control their data, including the ability to access, correct, or delete their data.
- We aim to minimize the processing of personal data to only process data necessary to achieve the related business purpose, use anonymized data in lieu of personal data where possible, and delete personal data no longer needed for the purpose for which it was collected, subject to legal retention requirements.
- We maintain specific policy controls related to how we share personal data, including when we transfer personal data across international borders.
- We apply appropriate organizational and technical security measures to protect personal data.

For additional information, please visit Morningstar's Privacy Center.

Our Preparedness

In order to effectively respond to any security incident, preparedness is a crucial component of our information security and privacy programs. All Morningstar employees

MORNINGSTAR®

complete an annual security awareness training. We also operate a quarterly phishing exercise to educate and test our employees. The security operations team conducts red team exercises to assess any ability to compromise our infrastructure and gain insight into our ability to detect and respond to an attack.

On a business level, we perform quarterly tabletop exercises to prepare all stakeholders for security incidents and practice our response procedures. Furthermore, our enterprise resilience team manages both disaster recovery as well as business continuity plans and prepares the firm to recover from high-impact incidents. Should an incident occur, we operate a 24x7 security operations team to respond to security incidents and notify relevant stakeholders.

Who is Responsible?

Morningstar has a dedicated Information Security team which is responsible for operating the firm's comprehensive information security program. The program and information security policies and standards align with ISO 27001 and the program's maturity is regularly evaluated against the NIST Cybersecurity Framework (CSF) to determine improvement opportunities. The program is led by the Chief Information Security Officer who reports to Chief Technology Officer and the Audit Committee of the Board of Directors.

Data in Our Products

Morningstar's product offerings may rely on personal data obtained from different sources, and the legal basis for processing personal data will vary depending on context. Our products designed for individual investors collect personal data directly from the customer and typically rely on opt-in consent. For our products designed for institutional customers, we may receive data relating to the institutions' customers, in which case we process personal data at the direction of the advisor and pursuant to contract. We also offer research products, such as PitchBook, which incorporate personal data that is publicly available or obtained from other third-party sources.

Where data is not collected from the customer or their representative, Morningstar typically relies on its legitimate interests as defined by applicable law and provides data subjects with required notice. In all cases, Morningstar will only process personal data as permitted by applicable privacy law.

Except as provided below, Morningstar only uses personal data as needed to deliver a product or service to a customer. Morningstar's research products, however, may distribute personal data that is relevant to its customers. For example, Morningstar subsidiary PitchBook publishes a limited set of data related to privately-owned company ownership (name, title, contact information), and Morningstar.com may publish personal data where newsworthy for Morningstar's investor customer base. Morningstar maintains data retention policies that balance legal retention requirements with Morningstar's own policy to maintain personal data only for as long as needed.

Due Diligence

Morningstar maintains processes to perform data protection impact assessments for new or changed data processing activities that potentially pose a high risk of harm to any natural person, including customers and employees. Morningstar policy requires the evaluation of the proposed processing activity considering applicable regulatory requirements, the necessity of the activity, the risks of the activity to data subjects, and the mitigating effect of safeguards. Morningstar's data protection impact assessment process applies to all processing activities, including activities performed by Morningstar personnel and activities performed by third parties. Morningstar recognizes that data security is not limited to data held within its own systems alone, but also includes data entrusted to partners and third-party service providers. In order to evaluate whether these entities have sufficient data protection controls in place, Morningstar operates a vendor due diligence process to evaluate the security practices of vendors.