HUNTON ANDREWS KURTH

Lawyer Insights

Privacy and Data Security in ESG

By Lisa Sotto, Aaron Simpson and Mike La Marca
Published in Corporate Counsel | March 15, 2022



Environmental, social and governance (ESG) standards have become crucial metrics for corporate performance, reputation and risk mitigation in recent years. Successful implementation of an ESG program not only affects a company's social and community profile, but also can positively influence its potential financial performance. Beyond well-known ESG issues covering carbon emissions, human capital development, responsible investing and business ethics, privacy and cybersecurity are fast becoming important topics for companies to address in their ESG programs and disclosures.

Recent analysis of public Form 8-K and Form 10-K filings over the past five years by Bloomberg Law confirms there has been a significant uptick in companies considering data privacy a noteworthy topic in their ESG-related statements. Likewise, in a 2021 survey of institutional investors by RBS Global Asset Management, cybersecurity was ranked as the second highest ranked ESG issue about which investors were most concerned, behind anti-corruption. Notably, MSCI, a leader in ESG ratings, includes privacy and data security as one of a few dozen key issues—among mainstays like climate change vulnerability, renewable energy, supply chain labor standards and community relations—in its ESG ratings framework.

ESG standards, which evaluate how a company performs according to certain socially relevant criteria (e.g., ecological impact and community well-being), are increasingly treating privacy and data security safeguards as significant indicators of corporate ethics that may not be captured in a traditional financial statement. Companies looking to help socially conscious investors understand their privacy and data security successes can leverage ESG standards in their sustainability or impact reports to highlight their strategies and practices. While companies may employ their own frameworks for evaluating their privacy and data security programs, third-party frameworks that help to standardize ESG measures across organizations also offer specific privacy and data security benchmarks. In addition, third-party ESG ratings that score companies' relative exposure to and management of privacy and data risks as compared to industry peers can influence socially responsible investment choices.

The Global Reporting Initiative (GRI) Standards is a third-party framework widely used by companies to assess their ESG performance within common categories and produce sustainability reports using standardized criteria. Accordingly, the GRI Standards are an important benchmark for understanding which privacy and data security factors companies are focusing on in their ESG disclosures. In particular, GRI has released a "Customer Privacy Standard," which provides an instructive guide.

Under the GRI standards, where a company considers customer privacy to be a "material topic" (i.e., a topic that reflects the company's significant economic, environmental and social impacts, or that

materially influences the assessments and decisions of its stakeholders), it must comply with prescriptive reporting requirements. Specifically, the report must include a narrative explanation of how the company manages customer privacy, its impacts and stakeholder expectations (i.e., the "management approach") and disclosures regarding specific privacy and data security issues contemplated by GRI (i.e., "topic-specific disclosures").

Management approach disclosures are required for all material topics identified by a company under the GRI framework. They must include certain content for each material topic, such as why the topic is material and descriptions of the organization's policies, commitments, goals and targets, responsibilities, resources, grievance mechanisms and specific processes and programs related to the topic. Management approach disclosures thus are primarily concerned with a company's governance and accountability mechanisms relating to privacy and data security and other material topics.

GRI customer privacy "topic-specific disclosures" provide a useful benchmark for companies seeking a general understanding of the types of additional considerations that factor into privacy-related ESG reporting. Under the GRI framework, customer privacy disclosures should address two broad but significant issues that focus on customer harm: the total number of substantiated complaints a company received regarding breaches of customer privacy (including from outside parties and regulators) and the total number of identified leaks, thefts or losses of customer data. Some companies will choose to provide these metrics in a separate index breaking down these numbers by year and other relevant categories (e.g., complaints from third parties versus complaints from regulatory bodies).

For lawyers accustomed to parsing specific definitions of terms such as "data security breach" under various global privacy and data security laws and regulations, it is important to note that the GRI customer privacy standard defines a "breach of customer privacy" not in terms of a data breach but rather in relation to "noncompliance" with legal regulations and voluntary standards regarding customer privacy. "Customer privacy," in turn, is defined broadly to include "matters such as the protection of data; the use of information or data for their original intended purpose only, unless specifically agreed otherwise; the obligation to observe confidentiality; and the protection of information or data from misuse or theft." Privacy and data security lawyers will recognize certain core fair information practice principles commonly found in global legal frameworks, such as "purpose limitation" and "security," imbedded in this definition of customer privacy.

Accordingly, a company's adherence to the GRI customer privacy reporting standard necessarily involves an understanding of a company's legal compliance posture with respect to relevant global privacy and data security laws. This may be particularly challenging for multinational companies, which must address rapidly evolving laws and regulations that may be interpreted and applied differently across jurisdictions and impose different, or at times conflicting, requirements. Beyond legal compliance, the GRI Standard's particular focus on data breaches—leaks, thefts or losses of customer data—is unsurprising given ever-growing concerns over the security of customer data amidst a dynamic cyber threat landscape. Privacy professionals should note, however, that the focus on unauthorized disclosures here is narrower in scope than most US state breach notification laws, which generally are more concerned with unauthorized *access* to or acquisition of personal information, not solely breaches that result in leakage, theft or loss.

In practice, companies' sustainability and impact reports can vary widely in terms of the degree of detail they provide related to privacy and data security. For example, where system security is integral to the

safety and reliability of a company's core product offerings, such as securing the software powering connected hardware (whether devices, appliances or vehicles), an impact report may focus more on cybersecurity, as in the cases of Tesla and GE. Companies with more detailed cyber disclosures often include a combination of general practices (such as vulnerability and security incident management), more specific practices (such as threat assessment and penetration testing) and use of relevant certifications and industry best practice frameworks (e.g., the National Institute of Standards and Technology Cybersecurity Framework, Open Web Application Security Project methodologies, the Payment Card Industry Data Security Standard and the ISO/IEC 27000 standard).

Where a company's core offering involves handling a significant amount of customer information—for example in connection with the provision of financial products or services or a widely-used ecosystem involving devices, operating systems and subscription services—a sustainability report, by contrast, may devote considerable attention to both privacy and data security as two key and interrelated concepts. For example, Mastercard and Apple make privacy a relative centerpiece of their disclosures, invoking it as a company priority, articulating philosophies related to the handling of personal information, and alluding to or invoking as notable features principles from global privacy regimes, such as transparency (which often includes a reference to a company's privacy notice), data subject rights and privacy by design. These companies also often address privacy and data security in parallel, with concepts such as encryption leveraged as both a privacy- and security-protective measure. Some companies also describe (in varying levels of detail) internal privacy programs that are based on comprehensive global privacy laws (e.g., the European Union's General Data Protection Regulation and the California Consumer Privacy Act). Such disclosures not only help address GRI's concern with instances of noncompliance but also demonstrate a company's commitment to robust privacy frameworks and methodologies premised on widely accepted principles.

Although ESG incentivizes disclosures regarding a company's privacy and data security successes, this should not be interpreted as a license to engage in puffery. The Federal Trade Commission (FTC), the primary federal privacy regulator in the United States, has authority to pursue "deceptive" trade acts or practices quite broadly, and the FTC has routinely relied on this authority to prosecute companies for misleading privacy and data security representations (both express and implied). Such representations are not necessarily limited to privacy policies or notices; the FTC also has focused on other public statements containing privacy and data security representations (e.g., blog posts) and conceivably could scrutinize ESG disclosures as part of an investigation or enforcement action related to deceptive conduct. Accordingly, it is important for companies to carefully vet statements regarding their privacy and data security practices in ESG reports to avoid potentially actionable misrepresentations.

Ultimately, in the face of growing demand in the market to satisfy ESG standards, companies that mishandle or ignore ESG risks and sustainability reporting face the additional risk of chilling investor confidence. As companies look to become leaders in ESG, the role of privacy and data security considerations will increasingly play a pivotal role.

Privacy and Data Security in ESG
By Lisa Sotto, Aaron Simpson and Mike La Marca
Published in Corporate Counsel | March 15, 2022

Lisa J. Sotto *chairs Hunton Andrews Kurth's global privacy and cybersecurity practice and is the managing partner of the firm's New York office. She can be reached at 212-309-1223 or lsotto@HuntonAK.com.*

Aaron P. Simpson *is a partner in the firm's global privacy and cybersecurity practice in the firm's New York office. He can be reached at 212-309-1126 or asimpson@HuntonAK.com.*

Michael La Marca *is a counsel in the firm's global privacy and cybersecurity practice in the firm's New York office. Michael can be reached at 212-309-1116 or mlamarca@HuntonAK.com.*