Technology has enabled unprecedented levels of data sharing, processing and analysis in modern life. While this has brought many benefits to people and businesses, recent years have also seen an increasing number of controversies over improper personal data usage. The conversation on privacy has moved far beyond the more technical legal and compliance spheres. The use of data to make determinations or predictions that affect individuals is a powerful and sometimes controversial ethical issue.

We are all likely to have different views on where these ethical boundaries should lie, but it is important for businesses to be able to explain to senior management, business partners, customers and regulators how they identify, understand and address any privacy risks and ethical considerations relating to their use of data.

Increasingly, corporates and investors recognise that to create and sustain long-term value it is important to consider the impact of business activities beyond purely financial indicators.[1] This is the core rationale behind environmental, social and governance (ESG) criteria, which are designed to guide assessments of companies’ purposes, activities, and likely future financial performance.

Companies are coming under more scrutiny than ever when it comes to the use of data. ESG may offer companies a way to measure performance in this area, demonstrate effectiveness and, above all, build sustainable value for all stakeholders.

**Privacy and data compliance in an ESG context**

The breadth of data usage in business means that privacy and data compliance now cuts across all corporate activities and sectors. Privacy and data management considerations also surface in each of the core ESG pillars.

The relationship is most obvious for governance. Ever-increasing privacy and data protection regulations around the world make it particularly important to maintain compliance in the processing and management of personal data. The EU General Data Protection Regulation (GDPR) specifically refers to the principle of accountability and the responsibility that organisations have to ensure that appropriate monitoring and controls are in place to demonstrate compliance with privacy commitments.

The roots of privacy and data protection law lie in human rights. All organisations need to consider the impact of technology and data processing on individuals, recognising individuals’ rights to privacy at home, at work, and to have their data collected and processed fairly and lawfully.

Advances in technology and science allow increasingly pervasive analysis of the way in which we live our lives. Algorithms determine creditworthiness and are used to carry out DNA testing. Taking into account the ethical implications of these activities is becoming an increasingly important consideration under ESG’s social pillar.[2]

Finally, there are non-trivial environmental considerations related to data use. These include energy consumption linked to data
centres and opportunities for data minimisation, and the appropriate deployment of energy-intensive data technologies such as blockchain.

**Moving beyond ‘compliance’**

The rationale for considering privacy and data compliance in ESG mirrors that of the movement more widely — taking a broad view of the impact of data usage can lead to better risk management and increased opportunities in the long term.

Companies with data issues face the potential for significant reputational damage, reduced valuations, and substantial regulatory sanctions. Governments are increasingly eager to retrospectively address perceived regulatory failings and keep pace with new data technologies and business models.[3] In this climate it is doubly important for businesses to consider their responsibilities, and potential exposure, above and beyond simply complying with existing legislation.[4]

**Benefits may include:**

- **Developing a forward-looking policy position on privacy and data compliance to guide long-term, sustainable data use.**

Companies that set privacy and data compliance goals linked to social and ethical considerations of their impact are likely to be in a better position to maintain consumer trust and navigate regulatory, political and cultural pressures.

Adopting this stance can also provide a rationale and framework to feed these considerations into wider data strategies, to assess the business value of compliance, and to develop enterprise-wide stances on digital ethics, AI governance and other data compliance-related topics gaining increasing attention.

- **Keeping privacy on the agenda**

Major regulatory developments such as the GDPR and the California Consumer Privacy Act (‘CCPA’) have kickstarted many large compliance programmes. Even after the big transformation projects related to new legislation end, it is important that organisations continue to dedicate budget and resources to privacy, building on solid foundations in order to keep pace with new regulatory demands.

Incorporating privacy into ESG and linking it to the wider company mission can help to make sure it retains visibility and receives the support, oversight and resources it deserves from senior management.

- **Make it measurable: integrating privacy goals into business activities**

Organisations that adopt a holistic approach to privacy and data compliance, and which build privacy concerns into business decisions early, are more likely to derive long-term benefits.

Making privacy and data compliance a measurable component of ESG goals will help to hold the business to account and keep the issue top of mind across the organisation. It can also provide management with meaningful information to guide their oversight of data use and inform strategic decision-making.

- **Delivering confidence in the global data supply chain**

Analysts view the complexity and risk in global value chains as a key driver for the ESG agenda. Data supply chains — often the source of serious data breaches or a focus area for regulators — are no exception.

In committing to privacy and data compliance, organisations’ ESG stances can help reassure corporate customers and business partners. Companies can also extend ESG expectations to vendors handling data on their behalf, enhancing confidence in data supply chains wherever in the world data is being processed or stored.

As greater importance is attached to this area, these benefits have the potential to become a competitive differentiator for businesses.
From theory to practice

While privacy and data are still emergent areas within ESG, there are some limited and formalised criteria in standards and ratings.[5] There is also a developing discussion on the societal impacts and ethics of data use.[6]

The devil at this stage is likely to be in the detail of developing a meaningful and proportionate approach for integrating privacy and data compliance into companies' ESG activities and securing the support of senior management.

Bearing in mind the wider aim of ESG to guide and serve overall corporate purpose, organisations will want to calibrate goals and measures in line with their risk appetites and data activities. Hopefully the discussion above highlights some potential advantages of taking action. There are clear opportunities for proactive companies to shape the development of this topic, but there are also risks to be aware of. Organisations will need to be careful that they are not exposing themselves to liability by committing to principles or standards that they fail to meet in practice.

Ideas for initial steps that companies can take to develop their stance in this area are:

1. Understand how privacy commitments and data usage can be factored into your existing ESG and sustainability assessments, and identify what aspects are most relevant to your corporate goals and stakeholder interests.
2. Set up or join an internal working group to bring relevant parts of your organisation into the discussion on privacy, data strategy and ESG.
3. Develop a corporate policy position and vision on privacy and data compliance, including key goals and commitments relevant to your business.
4. Engage with business partners, industry groups and subject-matter experts in privacy, data compliance, digital ethics and ESG to help align approaches and demonstrate commitment to this area.
5. Define key metrics to measure progress against your policy vision, determining how and when to incorporate insights into internal and public reporting.
6. Use third-party assessments or audits to monitor the effectiveness of relevant programmes and to provide insights into key priorities, industry/peer group benchmarking, public investor expectations, and to inform future activities.
7. Provide board-level briefings and training on privacy and data compliance.
8. If appropriate, consider establishing a committee of internal and external experts to assist in addressing complex data privacy and ethical issues in the context of business and technology transformation and related data strategy.


A&M's privacy and data compliance practice focuses on supporting clients to navigate the evolving and complex data protection regulatory landscape to develop and implement solutions to address these challenges.

We offer specialist advisory and consulting services on international and cross-border privacy, data protection, secrecy and related laws and sectoral rules. Professionals within the practice include former consultants, regulators, data protection officers and certified information privacy professionals who are skilled at aligning and implementing complex regulatory requirements within operational processes and settings.


See for example (a) the UN Principles for Responsible Investing (PRI) privacy-related considerations for cyber security under ‘governance’: https://www.unpri.org/governance-issues/stepping-up-governance-on-cyber-security/3452.article and, (b) the Global Reporting Initiative (GRI) sustainability reporting standard on customer privacy under ‘social’: https://www.globalreporting.org/standards/media/1033/gri-418-customer-privacy-2016.pdf

Source URL: https://www.alvarezandmarsal.com/insights/esg-and-privacy-foundation-better-compliance

Authors: