Leveraging Data Responsibly:

Why Boards and the C-Suite Need to Embrace a Holistic Data Strategy

April 2024

FOREWORD

At a time of unprecedented and profound digital transformation of our societies and economies, and with every organization now a digital and data-driven enterprise, the power and benefits of data are being felt beyond the confines of traditional technology companies. Public and private sector organizations of every size are recognizing the value of data beyond the operational and technical realities of digitized data and processes.

Data drives economic growth and efficiencies. It propels breakthroughs in science, health, and research. It energizes legitimate, innovative, and beneficial business purposes. Indeed, the explosive growth of generative AI has put in sharp focus the power of digitization and the value of data for proper development and functioning of AI.

At the same time, data and its use have become highly regulated, carrying compliance, commercial, and reputational risks. It is perhaps not surprising that corporate C-suites and Boards have traditionally focused on data through the lens of legal compliance, risk, and liability, putting it squarely within the purview of risk, audit, and governance committees.

Data is the one business asset that is not on corporate balance sheets, yet it is absolutely essential for business growth, competitiveness, and sustainability. To capitalize on this asset, companies will need to make a shift and consider data strategically, holistically, moving beyond traditional risk-and-compliance functions and across business silos. Companies will need to foster interdisciplinary conversations that consider and consolidate different business perspectives—engineering, information security, legal, ethics, compliance, and others. This holistic approach will bridge data silos at the structural, operational, and leadership levels to advance a single, coherent, organizational strategy that integrates the identification and management of data risks with the consideration and recognition of new data uses, innovations, and opportunities.

Indeed, the business case for adoption of AI technologies will further focus the need for this new integrated and holistic approach, as data powers the development and deployment of AI technologies. Importantly, a holistic data strategy enables organizations to navigate existing and new risks of datafication and digitalization, including AI, while reaping and delivering the benefits to multiple stakeholders.

Finally, a holistic data approach serves as a foundation for building digital trust by promoting responsible uses of data and responsible data-driven technologies. Moreover, it equips companies with the ability to respond to new disruptions, including the mounting digital regulation tsunami spanning the globe and the increasingly demanding expectations of customers, regulators, and investors.

Of course, setting the tone for this new strategy must come from the top. The Board of Directors is responsible for leading the initiative, and the C-suite must translate and implement it. A successful shift in corporate priorities and mindset cannot advance without alignment and collaboration from corporate leadership. To the extent the C-suite views data solely as a corporate liability/compliance issue, it is incumbent upon the Board to expand the corporate vision and focus the executive team on viewing data beyond the risk. Likewise, if the Board has a “data-as-a-liability” mindset, the executive team must articulate the invaluable role of data and the need for a data strategy that bridges traditional corporate silos and enables effective data use and innovation.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

I am excited to see this shift taking place. Many leading companies are revisiting their data and digital strategies, bridging silos, integrating cross-disciplinary controls and processes, and creating new data governance programs and oversight.

In this CIPL white paper, we propose a roadmap for building a holistic data strategy that seeks to align the Board and C-suite on data-driven initiatives and provide a framework for promoting innovative and responsible uses of data, including the development and deployment of powerful AI technologies. I am grateful for the invaluable insight and guidance provided by CIPL member companies, who are pioneering these new approaches to holistic data strategy and governance. We are at the beginning of the journey, and I look forward to exploring and sharing best practices for corporate leadership and Boards to help support this transformation.

Bojana Bellamy

President
Centre for Information Policy Leadership

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

TABLE OF CONTENTS

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

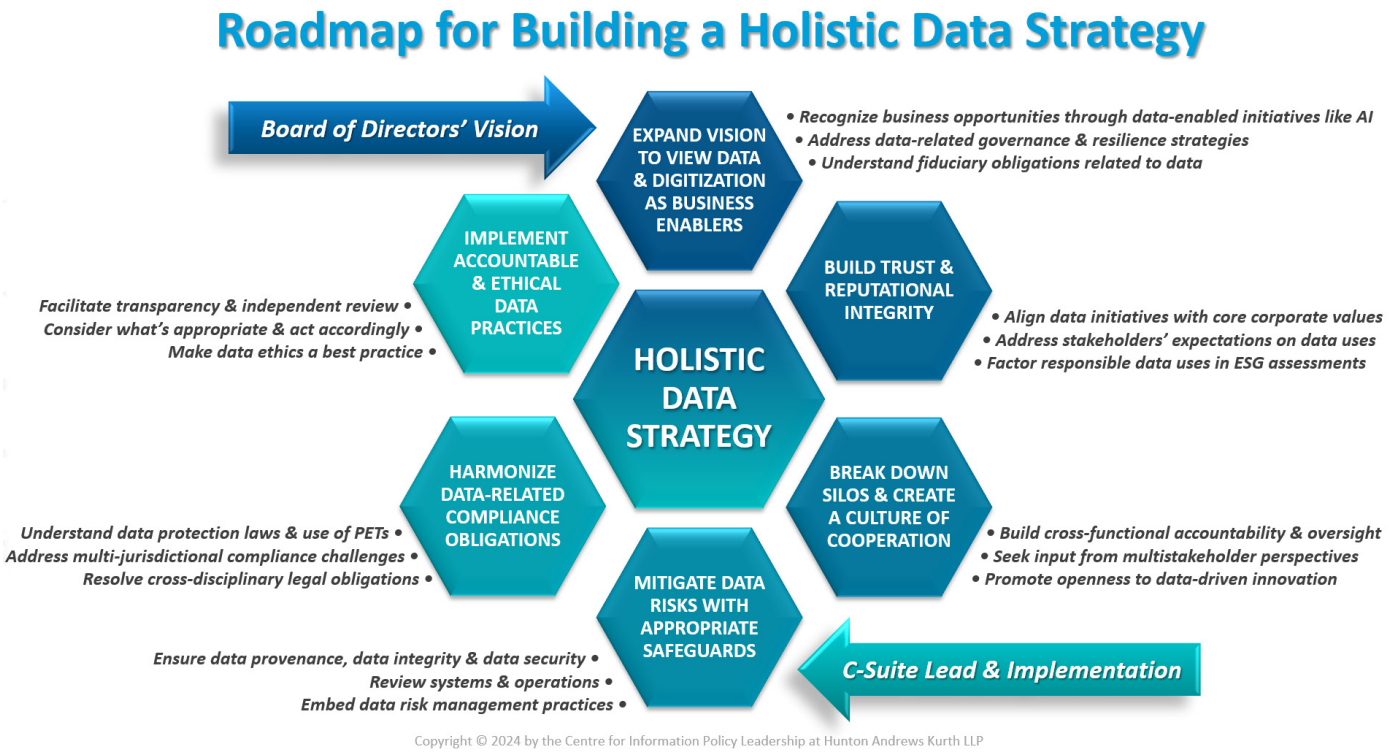
Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EXECUTIVE SUMMARY

Because most data protection laws focus on personal data—i.e., data that can identify or lead to the identification of an individual—businesses accustomed to addressing data privacy and security issues may think of data only in terms of what is personally identifiable. But business data, of course, comprises much more than individual names, email addresses, and other types of personally identifiable information. Data used by AI technologies, for example, is by no means restricted to personal information. Indeed, legislators and regulators (especially in Europe) are looking at data with a broader perspective, viewing all data collected and generated by business as a market differentiator and a key factor for economic and productivity growth. Thus, to embrace a **holistic data strategy**, companies must first move beyond an individual or consumer privacy focus by looking at information of all types, including personal, non-personal, meta, derived, inferred, and aggregate data.

While uses of data certainly trigger legal obligations and potential risks, businesses that have adopted a holistic data strategy can address those obligations and assess those risks before green-lighting a particular initiative, including initiatives that embrace AI. While each organization presents different challenges, a holistic data strategy can be adopted regardless of size and sector.

CIPL proposes the adoption of the following roadmap for the development of a holistic data strategy that can be tailored to the needs of any organization, with the Board of Directors setting the vision and the C-suite leading and implementing a framework to enable specific proposals. The infographic pictured below displays shades of blue and green to visualize the overlap between Board (blue) and C-suite (green) responsibilities, with shade variants emphasizing where respective duties primarily lie.



Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

CIPL's colorful roadmap therefore envisions a dynamic process for fostering and weighing new uses of data that could identify new business opportunities or enhance existing products and services, help evaluate a potential merger or acquisition, promote more effective operations and customer engagement opportunities, or deploy a new AI-powered application. It comprises six core steps:

1. Expand vision to view data and digitization as business enablers

Since the Board is primarily responsible for setting corporate goals and strategy, Board members should be the ones charged with re-examining the corporate vision and assessing the opportunity for growth through responsible uses of data. Sometimes, however, Board members are not able to see data and digitization as business enablers. If that's the case, companies will need to ask: What are the best strategies for getting the Board to understand the essential role of data for the organization and how to get the Board "on board" with a strategic approach to data? How can the Board and executive leadership align on a corporate vision that understands data as an asset?

The goals of the first step are to:

- Recognize business opportunities through data-enabled initiatives like AI
- Address data-related governance and resilience strategies
- Understand fiduciary obligations related to data

2. Build trust and reputational integrity

A holistic approach takes into consideration important reputational and societal factors, including those that factor into Environmental, Social, and Governance (ESG) initiatives. In addition to the more frequently cited environmental and governance elements of data, many companies are now recognizing a social responsibility to be respectful of personal and behavioral data. While stakeholders' expectations regarding a specific use may differ, in the end, organizations must seek to earn their trust. Here, companies will need to ask: Would customers, regulators, and other stakeholders be surprised, annoyed, disillusioned, or frustrated to learn of the company's proposed uses of data?

The goals of the second step are to:

- Align data initiatives with core corporate values
- Address stakeholders' expectations on data uses
- Factor responsible data uses in ESG assessments

3. Break down silos and create a culture of cooperation

Breaking down corporate silos is key to developing a holistic strategy, so data initiatives must invite stakeholders from different business units to share their knowledge and perspectives on current and proposed uses of data, and to discover how each can benefit from and leverage institutional and business line knowledge. Here, companies should ask: How is cross-departmental communication fostered and which perspectives need to be addressed?

The goals of the third step are to:

- Build cross-functional accountability and oversight
- Seek input from multistakeholder perspectives
- Promote openness to data-driven innovation

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

4. Mitigate data risks with appropriate safeguards

Risk is inherent in all business decisions, so companies must discern ways to identify and mitigate data risks while recognizing the benefits of moving forward and embracing innovation and opportunities. An assessment of security safeguards is key, and organizations will need to factor in the cost of any residual risk. Since new uses of data are only as good as the underlying data sets, companies will need to adopt practices that validate the accuracy of the data and the reliability of data sources. This is especially crucial in the AI context. Here, companies should ask: What sorts of practices can ensure data integrity and trustworthiness? Does the business have adequate safeguards in place to protect its digital assets? How should corporate leaders fulfill their oversight duties and minimize the risks associated with data-driven business decisions?

The goals of the fourth step are to:

- Ensure data provenance, data integrity, and data security
- Review systems and operations
- Embed data risk management practices

5. Harmonize data-related compliance obligations

At this part of the strategy, compliance takes center stage, with special emphasis on the data protection and localization obligations associated with certain data types and data uses. Increasingly, however, companies must harmonize those obligations with other equally important legal considerations, such as antitrust and competition concerns. In the case of AI, intellectual property, bias, discrimination, and other issues come into play. Here, companies should ask: What are the key obligations and responsibilities regarding the data at issue and what potential conflicts must be addressed?

The goals of the fifth step are to:

- Understand data protection laws and use of PETs
- Address multi-jurisdictional compliance challenges
- Resolve cross-disciplinary legal obligations

6. Implement accountable and ethical data practices

A holistic data strategy takes into account considerations of data ethics when organizations use data to enhance or develop their services and technologies. Ethical considerations—which are strongly related to concepts embedded in data protection laws (such as fairness, transparency, proportionality, and accountability)—can help organizations assess whether a proposed purpose or means of processing is acceptable or not. Indeed, the establishment of an ethical oversight committee is rapidly becoming recognized as best practice in the development and deployment of AI technologies. Here, companies should ask: Is this the right thing to do? Can we do better?

The goals of the sixth step are to:

- Facilitate transparency and independent review
- Consider what's appropriate and act accordingly
- Make data ethics a best practice

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

STEP ONE

1. EXPAND VISION TO VIEW DATA & DIGITIZATION AS BUSINESS ENABLERS

A. Recognize business opportunities through data-enabled initiatives like AI

Legislators and regulators around the world increasingly view data practices through a market competition lens,[1] yet many Boards still assign internal review of data-related issues to a governance, audit, or risk committee. Boards of Directors need to recognize data for what it has become in our digitized economy: the fuel of the digital economy and a critical business asset to be considered through a strategic lens. Boards must especially be cognizant of the responsible development and use of AI.[2]

Why the Board? Generally speaking, the Board of Directors of a company is primarily responsible for:

- determining the company's strategic objectives and policies;
- monitoring progress towards achieving those objectives and policies;
- appointing senior management; and
- accounting for the company's activities to relevant parties (e.g., shareholders).[3]

Since the Board sets the direction for the future of the company, it should identify opportunities for growth and innovation, like AI. It is therefore incumbent upon the Board to expand the corporate vision and inquire about ways to leverage data—a principal corporate asset—especially where the C-suite is viewing data solely as a corporate technology/liability/compliance issue.

Of course, the Board itself may recognize the opportunity for growth, but liability risks may stifle its verve to innovate. That's when the executive team must articulate the need for a data strategy that

---

1 See, for example, the recently adopted EU Digital Markets Act, which seeks to promote competition in the digital sector by curbing the market power of large digital platforms acting as gatekeepers.

2 See Richard Milne, *Norway's oil fund is sending a message to companies on AI*, Financial Times (Sept. 7, 2023), available at https://www.ft.com/content/52df2867-c955-4389-84c6-33c091e9c1dd.

3 Directors' Duties, The Chartered Governance Institute UK & Ireland, available at https://www.cgi.org.uk/professional-development/careers/directors-duties.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

bridges traditional corporate silos and enables innovation. Indeed, the C-suite and the Board need to be aligned to drive an effective data strategy.

i. Data as business enabler

Enabling the shift to a data-driven strategy can be particularly difficult for organizations that were not "born digital" or not otherwise familiar with leveraging data insights.[4] The following points can help to convey data's broad value:

- *Data is more than personal information*

Given the notoriety of laws like the EU's General Data Protection Regulation, businesses accustomed to addressing data privacy and security issues may think of data only in terms of what's personally identifiable, which in turn reinforces the idea that data is solely a risk-and-compliance issue.

But business data, of course, comprises much more than customer names, addresses, and other types of data relating to a natural person. For example, marketing departments collect data that tracks click-through rates in email marketing campaigns. Finance departments track expenditures by type and frequency. Logistics departments track inventory levels at various warehouses.

Businesses, therefore, need to adopt a broader view of data that includes all types, regardless of whether it is deemed personal, non-personal, meta, derived, inferred, aggregate, or otherwise. And they need to make connections between seemingly disparate sets of data, supplemented with additional information. If click-through rates remain unchanged after the sales team expensed regional luncheons for potential customers, the company may want to collect other sets of data (such as the timing of the emails and the locations of the lunches) before reaching a conclusion on the utility of hosting luncheons. Data about seasonal buying trends of particular products or specific events can inform when manufacturing needs to be stepped up or down, and supply chains readied accordingly.

- *Data is expanding and is multi-faceted*

Data is the natural by-product of the digitization of the economy. Individuals gain access to offices and hotel rooms with the swipe of a badge. Packages are scanned from shipment to delivery. Menu items are ordered on a touch screen. Nearly every transaction is digitally recorded in some way, creating a trove of datasets that can provide insights into markets, trends, and costs.

The Future of Jobs Report,[5] released by the World Economic Forum in October 2020, listed data analysts and scientists, AI and machine learning specialists, and big data specialists as the leading positions growing in demand. And that's no surprise: The profusion of data fuels a demand for employees who can gather, interpret, and repurpose data to advance business objectives.

---

[4] One notable exception is the automobile manufacturing industry, which has embraced data as a business asset through the evolution of smart cars and in-car data analytics that affect the full breadth of the sector from safety to maintenance to car design. See Ed Garsten, Auto Software, Data Innovations Are Now Shadow Vehicle Powertrain, Forbes, Jun. 12, 2023.

[5] WEF, *The Future of Jobs Report 2020*, https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

- *Data is strategic, fuels innovation, has value*

As mentioned above, data is being eyed by legislators and regulators as essential to a vibrant digital economy. The EU's Digital Markets Act,[6] which entered into force 1 November 2022, seeks to promote competition in the digital sector by, among other things, allowing business users of so-called "gatekeeper" platforms to access the data they generate while using the platform. Specifically, it requires gatekeepers to provide business users with "effective, high-quality, continuous and real-time" access and use of aggregated and non-aggregated data, including personal data.

The EU's Data Act,[7] which entered into force 11 January 2024, allows users of connected devices to gain access to data generated by them, i.e., data otherwise harvested (and retained) by IoT manufacturers and service providers. Notably, the legislation permits users to share that data with third parties, who would then be able to provide aftermarket and other value-added services.

Proposed legislation in the U.S. similarly seeks to reduce the market power of data aggregators. See, for example, proposed bills such as the Digital Consumer Protection Commission Act,[8] the Open Apps Market Act,[9] and the American Innovation and Choice Online Act.[10]

Together these new and proposed measures mean that organizations otherwise hesitant to address data governance from a business opportunity perspective may nevertheless need to navigate additional legal and regulatory obligations.

Moreover, organizations should understand that advances in digital analytics can support strategic decision-making, enabling them to:

- reduce bias in decision-making by calibrating the likelihood of a strategy's success before allocating resources;
- unearth new growth opportunities by revealing hidden pockets of potential growth;
- identify early-stage trends by painting a real-time picture of what's unfolding in order to trigger moves before competitors; and
- anticipate complex market dynamics by generating proprietary insights about the combined impact of various market forces.[11]

The Organisation for Economic Co-operation and Development (OECD) has identified data-driven innovation (DDI) as a "key pillar in 21st century sources of growth."[12] While acknowledging that the analysis and use of data is not new, the OECD recognizes that a confluence of three major socio-

---

6 Digital Markets Act, available at https://competition-policy.ec.europa.eu/dma_en.

7 "Data Act enters into force: what it means for you," available at https://commission.europa.eu/news/data-act-enters-force-what-it-means-you-2024-01-11_en.

8 Digital Consumer Protection Commission Act, S.2597, 118th Congress, available at https://www.congress.gov/bill/118th-congress/senate-bill/2597.

9 Open App Markets Act, S.2710, 117th Congress, available at https://www.congress.gov/bill/117th-congress/senate-bill/2710; H.R.5017, 117th Congress, available at https://www.congress.gov/bill/117th-congress/house-bill/5017.

10 American Innovation and Choice Online Act, S.2033, 118th Congress, available at https://www.congress.gov/bill/118th-congress/senate-bill/2033.

11 Chris Mulligan, et al, *The strategy-analytics revolution*, McKinsey & Company, April 6, 2021, available at https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/the-strategy-analytics-revolution.

12 OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://doi.org/10.1787/9789264229358-en.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

economic and technological trends has made DDI a new source of growth: (1) the exponential growth of data generated and collected; (2) the power of data analytics; and (3) the use of data to drive decisions.[13]

On the third point, the OECD's report highlights that decision-making is increasingly based on real-time monitoring and overwhelmingly made with the use of machine learning and automated decision-making technologies.[14]

While some would like to distinguish DDI from data-driven optimization (DDO) and data-based innovation (DBI),[15] CIPL finds such distinctions irrelevant for the purpose of highlighting the importance of data to the Board and senior leadership. If a Board recognizes that data can optimize efficiency (DDO) or enhance the utility of products or services (DBI), the Board's recognition of data as a business-enabler is not far behind.

ii. Getting buy-in from the Board

a. Know your audience

To encourage corporate leadership to view data as a business enabler, a good first step is to know your audience. How has the Board been briefed on data-related issues in the past? Have these issues been addressed solely in a risk-and-compliance report? Have they been discussed only in the context of a data breach?

If the Board's experience with data has been limited to such contexts, it is best to address the Board's likely (and legitimate) concerns head-on. The Chief Privacy Officer (or someone similarly equipped with knowledge of the risks inherent in certain uses of data) should acknowledge that data-related compliance is a necessary cost of doing business and that irresponsible and unethical uses of data can and do lead to legal liability and reputational damage. Of course, the CPO should also highlight the other side of the coin: data opens new opportunities and inspires innovation, providing a springboard for the Board's vision and strategy.

Indeed, proactively addressing data privacy issues that raise legal and reputational harm has become a business imperative. According to an article published by the Nasdaq Center for Board Excellence, profitable companies have made data privacy and security their brand differentiators.[16] In 2022, the ten largest companies by revenue have gone on the record with commitments to protect consumer privacy and security, and leaders of leading technology companies have advocated for the positioning of privacy as a business imperative.

A joint report from CIPL and the Privacy Center of Excellence at Cisco[17] confirms this trend, noting that organizations are increasingly discussing privacy with top management in the context of a broader data strategy. Even more, the report, published in January 2023, recognizes that companies

---

13 *Id.*, at p. 134.

14 *Id.*, at p. 150.

15 Luo, Jianxi, *Data-Driven Innovation: What Is It?* (December 15, 2021), available at https://ssrn.com/abstract=3951983.

16 Dominique Shelton Leipzig, *Data Privacy: A Business Imperative for Boards & Leaders That May Contribute to Market Recovery* (June 29, 2022), Nasdaq Center for Board Excellence, available at https://www.nasdaq.com/articles/data-privacy%3A-a-business-imperative-for-boards-leaders-that-may-contribute-to-market.

17 Cisco-CIPL Report on Business Benefits of Investing in Data Privacy Management Programs, Jan. 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cisco-cipl_report_on_business_benefits_of_investing_in_data_privacy_management_programs__10_jan_2023_.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

are realizing a return on investment (ROI) from data privacy management programs (DPMPs). Benefits include greater agility and innovation, operational efficiency, and investor interest.

b. Emphasize core values

Having anticipated and acknowledged the Board's risk-and-compliance concerns and having identified the ROI opportunities of good data governance practices, a CPO seeking to highlight the potential value of data should know what triggers the Board's attention. Oftentimes, it could be an appeal to the organization's core values, sometimes referred to as the "North Star." Data is the critical driver of setting, measuring, and reporting on an organization's core values, whether that be high-quality service, customer-first, integrity and respect, safety, efficiency, etc. Of course, where companies are undergoing a digital transformation, those core values may need to be re-cast in the light of that transformation.

c. Frame within ESG

Some organizations have advanced holistic data strategies via company-endorsed **Environmental, Social, and Governance (ESG) initiatives**. Forward-thinking Boards have come to recognize their dual obligations to shareholders and to society at large, and given the societal impact of modern data uses, some Boards have started to address data-related issues within the ESG context.

Of course, data is essential to establishing goals and measuring benchmarks for the 'E' of ESG. For example, companies measure carbon emissions with data relating to travel, logistics, and operations. And companies measure energy efficiency with data relating to system needs and occupant demands. Even though such data is not *personal*, highlighting tangible benefits derived from non-personal data is a good way to get Boards accustomed to viewing data holistically. Indeed, framing data in its broadest sense and without distinction is the foundation for envisioning data as a business enabler.

To advance specific "business enabler" initiatives, organizations have had success focusing on the 'S' and 'G' of ESG by highlighting their **social** obligation to be respectful of personal and behavioral data[18] and their **governance** obligation to develop responsible and ethical data practices.[19]

Moreover, because ESG is often tied to capital allocations, presenting data issues in the ESG context can sometimes provide funds for data-related initiatives.

iii. Porsche Case Study

The German car maker Porsche is developing privacy settings in its luxury cars as part of a **Board-approved strategy** to expand consumers' trust.[20] Christian Völkel, Porsche's chief privacy officer, is quoted as saying: "It's not our business to sell data and to make money out of the data of our customers. It's our business aim to make better services and products out of the data."[21]

---

18 Addressed in Section 2.C.

19 Addressed in Section 6.

20 Catherine Stupp, *Porsche Rolls Out Board-Approved Privacy Strategy*, WALL STREET JOURNAL, May 20, 2022, available at https://www-wsj-com.cdn.ampproject.org/c/s/www.wsj.com/amp/articles/porsche-rolls-out-board-approved-privacy-strategy-11653039001#.

21 *Id.*

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

The company's press release on its privacy strategy (dubbed "Privacy – Accelerating Dreams & Innovation") expressly states that it strives to "go beyond meeting compliance standards."[22] Indeed, the company's stated objective of the initiative is "to combine data-driven innovation, the ethical handling of data and compliance with legal requirements."[23]

B. Address data-related governance and resilience strategies

i. Corporate governance

Technology is changing so quickly that even leading practitioners are revisiting long-held assumptions about aspects of data governance. For example, McKinsey published an important article in 2021 entitled "How Boards Can Help Digital Transformations."[24] Among the suggestions highlighted was that Boards understand the *implications* of technology, not necessarily the technology itself. Citing AI as an example, the article suggested that Boards need not understand how AI works per se, but how it can unlock new revenue streams and increase competitive advantage.

The explosive growth of generative AI has left many companies uneasy with this notion of using technology without understanding it well—a pivot that McKinsey acknowledged in a 2023 article:[25]

> Unless board members understand generative AI and its implications, they will be unable to judge the likely impact of a company's generative AI strategy and the related decisions regarding investments, risk, talent, technology, and more on the organization and its stakeholders.[26]

Furthermore, the rise of generative AI does not change companies' fiduciary duties and responsibilities to assess and address risk.[27] Board members' fiduciary duties are discussed in greater detail in Section 1.C., below. CIPL's report on accountable AI governance[28] explores in greater detail how companies are navigating these challenges, while our *Ten Recommendations for AI Regulation* suggests steps governments can take to foster good practices.[29]

---

22 Privacy as a competitive advantage, December 3, 2021, available at https://newsroom.porsche.com/en/2021/company/porsche-data-protection-competitive-advantage-christian-voelkel-26665.html.

23 *Id.*

24 *How boards can help digital transformations*, by Celia Huber, Alex Sukharevsky, and Rodney Zemmel. McKinsey Executive Briefing, June 21, 2021, available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/how-boards-can-help-digital-transformations.

25 *Four essential questions for boards to ask about generative AI*, by Frithjof Lund, Dana Maor, Nina Spielmann, and Alexander Sukharevsky, McKinsey, July 7, 2023, available at https://www.mckinsey.com/capabilities/quantumblack/our-insights/four-essential-questions-for-boards-to-ask-about-generative-ai,

26 *Id.*

27 *Generative Artificial Intelligence and Corporate Boards: Cautions and Considerations*, by Lawrence A. Cunningham, Arvin Maskin and James B. Carlson, Mayer Brown LLP, Harvard Law School Forum on Corporate Governance, June 21, 2023, available at https://corpgov.law.harvard.edu/2023/06/21/generative-artificial-intelligence-and-corporate-boards-cautions-and-considerations/.

28 CIPL White Paper, *Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework*, February 21, 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_building_accountable_ai_programs_23_feb_2024.pdf.

29 CIPL, *Ten Recommendations for Global AI Regulation*, October 4, 2023, available at cipl_ten_recommendations_global_ai_regulation_oct2023.pdf (informationpolicycentre.com).

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Aside from the challenges of generative AI, there is increasing recognition among organizations that implementation of a data privacy management program (DPMP) is essential to operate effectively in the digital economy. The CIPL-Cisco report mentioned above[30] shows that a DPMP can enable a company to use and share data more broadly, including for data-driven innovation. The report also notes that more organizations are discussing privacy with top management in the context of a broader data strategy, communicating how a DPMP can create value for the company itself as well as for customers.

ii. Corporate resilience

Boards are also responsible for ensuring that the company is prepared for a wide range of potential crises, both unforeseen (like Covid-19) and predictable (like data incidents).[31] While most Boards already ensure that an incident response plan is in place, the Board's data resilience strategy should not be limited to addressing data intrusions and attacks. Boards should explore how corporate data uses and data policy can mitigate risks in times of crisis. For example, where geopolitical risk is a perennial threat, the Board should encourage the adoption of data storage and transfer practices that do not place data in unstable or potentially hostile jurisdictions.

C. Understand fiduciary obligations related to data.

The structure of the Board can vary depending on the type of company and jurisdiction. Increasingly, however, directors (including non-executive directors) are understanding their broader fiduciary obligations in the context of data as a business asset and data-driven decision-making. Shareholders and third parties are demonstrating their willingness to hold Boards to account in the context of data breaches, decisions, use, and governance, as indicated below.

i. Caremark

In the United States, Directors and Officers have a legal **duty of care** to act on an informed basis, a **duty of loyalty** to the corporation, and a **duty to act in good faith**.[32] In particular, the responsibilities of Board members stem from a 1996 decision from the Delaware Court of Chancery known as *Caremark*,[33] which requires directors to exercise a "**good faith effort**" to implement and monitor a reasonable system of internal controls. Directors can be liable for a breach of this oversight duty where three criteria are satisfied:

- the Directors knew or should have known that violations of the law were occurring;
- the Directors took no steps in a good faith effort to prevent or remedy that situation; and
- such failure proximately resulted in the losses complained of (i.e., the harm to owners/shareholders was a direct and foreseeable result of the violations of law and the Directors' failure to address it).[34]

So-called "*Caremark* claims" are among the most difficult for plaintiffs to bring. To prevail, a plaintiff must plead particularized facts showing that either (1) the Directors utterly failed to implement any

30 See note 17.

31 *The role of boards in fostering resilience*, Inside the Strategy Room Podcast, McKinsey, June 9, 2021, available at https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/the-role-of-boards-in-fostering-resilience.

32 Bloomberg Law, Portfolio 560: Cybersecurity Governance: A Guide for Corporate Officers, Directors and General Counsel, available at https://www.bloomberglaw.com/product/corporate/document/XOEV9A18.

33 *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

34 Bloomberg Law, Portfolio 560, *supra*, note 32.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

reporting or information system or controls or (2) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.[35]

While Delaware law imposes on Directors a duty to ensure that Board-level monitoring and reporting systems are in place, Directors also need to make a "good faith effort" to ensure the company has a system or controls in place. Arguably, a holistic data strategy would fulfill that requirement.

ii. Sullivan

Senior leadership accountability reached a new level—that of criminal liability—when a former CSO was found guilty in October 2022 by a jury in U.S. federal court for his failure to disclose a breach to the FTC in the midst of an ongoing FTC investigation.[36] Ex-CSO Joseph Sullivan was charged with one count of obstructing an FTC investigation and one count of misprision of a felony (i.e., concealing a felony from authorities). The case represents the first instance of a company executive facing criminal prosecution related to the handling of a data breach.

iii. Drizly

Senior leadership accountability went even further pursuant to an FTC consent order against an online alcohol ordering and delivery service, known as Drizly, and its CEO James Cory Rellas.[37] While it is not unusual for a consent order to apply to a company's operations for years to come, the *Drizly* order binds Rellas personally for the next 10 years, even if he leaves Drizly for another company.

The FTC's action arose from alleged failure to maintain appropriate security safeguards that led to a data breach affecting 2.5 million consumers' personal information. With regard to Rellas personally, if he joins another company that collects consumer information from more than 25,000 individuals as either a majority owner or a senior officer with "direct or indirect" responsibility for information security, the order requires him to ensure **within 180 days** that the new company "has established, implemented, and thereafter maintains, a comprehensive information security program."[38] The FTC noted in its press release that its unprecedented action was "part of the FTC's aggressive efforts to

---

35 *Stone v. Ritter*, 911 A.2d 362, 370 (De. 2006). See also *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019), which offers important guidance for directors in establishing Board-level oversight and prioritizing key risks. See generally, Board Oversight: Why Directors Must Care About Caremark, Hunton Andrews Kurth Client Alert, August 2019, available at https://www.huntonak.com/images/content/5/9/v2/59181/Board-Oversight-Why-Directors-Must-Care-About-Caremark_UpdatedSe.pdf.

36 *Former Chief Security Officer of Uber Convicted of Federal Charges for Covering Up Data Breach Involving Millions of Uber User Records*, Press Release, U.S. Department of Justice, Oct. 5, 2022, available at https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach. See also, *Former Uber Security Chief Found Guilty in Criminal Trial for Failure to Disclose Breach to FTC*, Privacy & Information Security Blog, Hunton Andrews Kurth LLP, Oct. 6, 2022, available at https://www.huntonprivacyblog.com/2022/10/06/former-uber-security-chief-found-guilty-in-criminal-trial-for-failure-to-disclose-breach-to-ftc/.

37 *FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers*, FTC Press Release, Oct. 24, 2022, available at https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million.

38 *In re Drizly LLC*, Decision and Consent Order, p. 10, available at https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

ensure that companies are protecting consumers' data and that careless CEOs learn from their data security failures."[39]

iv. SEC Cybersecurity Disclosure Rules

In July 2023, the U.S. Securities and Exchange Commission (SEC) adopted new cybersecurity disclosure rules for public companies.[40] The new rules apply to U.S. domestic public companies, as well as to any offshore company that qualifies as a "foreign private issuer" under SEC rules due to a strong nexus to the U.S. capital markets. The new rules became effective Sept. 5, 2023.[41]

Although the proposed version of the rules[42] would have required disclosure about the **cybersecurity expertise** of members of the Board of Directors, the final rules contain no requirement to identify a Board cybersecurity expert. Nevertheless, CIPL recommends that Boards include members with cybersecurity and data protection experience as part of their implementation of a holistic data strategy. A 2023 survey of CIPL member companies[43] reveals that nearly 60% have at least one Board member with experience or expertise in data privacy and/or data security issues.[44]

39 *Supra*, note 37.

40 SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, Press Release, July 26, 2023, available at https://www.sec.gov/news/press-release/2023-139.

41 "The final rules are effective September 5, 2023. With respect to Item 106 of Regulation S–K and item 16K of Form 20–F, all registrants must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. With respect to compliance with the incident disclosure requirements in Item 1.05 of Form 8–K and in Form 6–K, all registrants other than smaller reporting companies must begin complying on DECEMBER 18, 2023. As discussed above, smaller reporting companies are being given an additional 180 days from the non-smaller reporting company compliance date before they must begin complying with Item 1.05 of Form 8–K, on June 15, 2024." Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Final Rule), 88 FR 51896, 51924 (Aug. 4, 2023), available at https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

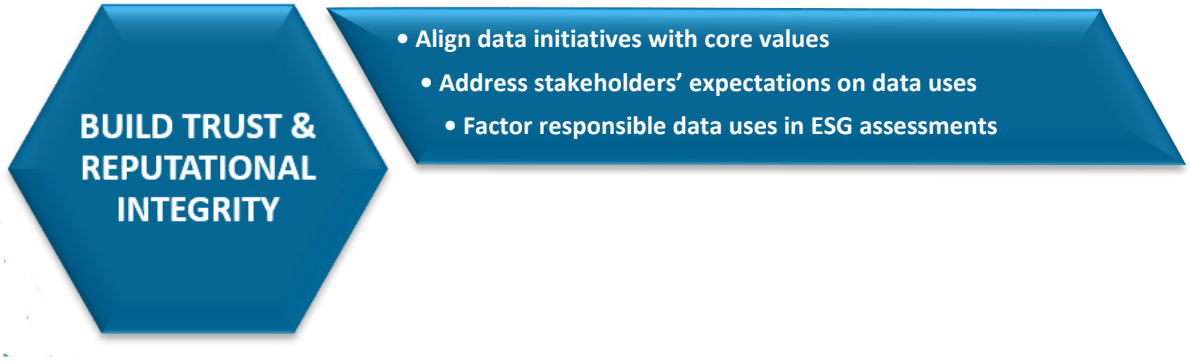
42 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Proposed Rule), 87 FR 16590, March 23, 2022, available at https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

43 The survey was conducted in September 2023, and the results are compiled in the Appendix.

44 See Results of CIPL Member Survey, Appendix, Question 12.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

STEP TWO



2. BUILD TRUST AND REPUTATIONAL INTEGRITY

A. Align data initiatives with core corporate values

To advance a holistic data strategy initiative, the corporate Board and the C-suite need to align on the mission, which ideally should be direct and succinct.

Porsche's strategy (highlighted in Section 1.A.iii.) serves as a good example. Its corporate press release[45] clearly underscores not only that privacy will take a principal role in the development of Porsche's future products and services, but also that the Board and the C-suite are equally committed to the initiative. Notably, the press release is written by the CPO and includes supportive comments from the deputy chairman of the Board. With messaging from the top aligned, a holistic data strategy can more easily permeate throughout the company, especially to those who are charged with implementing it.

Importantly, Porsche's statement underscores that its strategy aligns with corporate values by advancing innovation and focusing on the customer: "Porsche believes in the future viability of privacy, including as a competitive advantage, and will communicate privacy to its customers both boldly and with a pioneering spirit."[46]

B. Address stakeholders' expectations on data uses

Different stakeholders have different expectations. Shareholders expect data-driven initiatives to boost earnings. Regulators expect compliance with legal requirements. Customers expect uses of their data to be generally reasonable, easily explainable, and tangibly beneficial to them. Reasonableness, explainability, and beneficial impact are the keys to building consumer trust. As noted by Porsche: "[T]rust in the brand should be characterized not only by the quality of the

45 Privacy as a competitive advantage, December 3, 2021, available at https://newsroom.porsche.com/en/2021/company/porsche-data-protection-competitive-advantage-christian-voelkel-26665.html.

46 *Id.*

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

products and services, but also by the positive feeling enjoyed by customers who are firmly in control of their own data."[47]

C. Factor responsible data uses in ESG assessments

As noted in Section 1.A.ii.c., some organizations have brought holistic data strategies to the attention of the Board within the context of ESG initiatives. But beyond using ESG as an avenue to get buy-in from the Board, ESG may serve to boost a company's reputation as a **trusted data steward**. *CPO Magazine* has noted:

> Companies now have a **social responsibility** to be respectful of personal and behavioral data. They must weigh their reputation and investor benefits from prioritizing ESG against profits derived from third-party data collection and use. By positioning **privacy as a social value**, companies build a level of trust from society's expectation of privacy that had been lost. By being more scrupulous with data collection, consumers will feel comfortable sharing personal and sensitive information that will eventually build brand reputation and convert into investor-friendly profits.[48]

Formalizing processes for complying with individuals' data rights also forms an important part of the social impact of data. And ethical data practices (discussed *infra* in Section 6) also factor into societal benefits by generating trust from consumers and regulators alike.

Moreover, **governance** issues strike at the core of a holistic data strategy by requiring coordination and collaboration among traditionally siloed competencies—legal, compliance, information security, finance, engineering, risk, audit, ethics, etc. Indeed, more than half (54%) of respondents to CIPL's Member Survey have indicated that their organizations are viewing (or starting to view) data governance issues through the lens of ESG.[49]

That said, data stewardship issues do not currently appear to be factored into most third-party ESG assessments, and if they are, their significance is minimal at best. The Dow Jones Sustainability Index, for example, scores ESG risk from data provided by RepRisk, an ESG data science firm.[50] RepRisk, in turn, bases its research on 28 separate ESG issues, only one of which makes a passing reference to privacy.[51]

---

47 *Id.*

48 Sean Song, *Why Business Leaders Must Incorporate Data Privacy Into ESG Frameworks*, CPO Magazine, June 29, 2022, available at https://www.cpomagazine.com/data-privacy/why-business-leaders-must-incorporate-data-privacy-into-esg-frameworks/ (emphasis added).

49 See Results of CIPL Member Survey, Appendix, Question 8.

50 Dow Jones Sustainability Indices Methodology, p.21, available at https://www.spglobal.com/spdji/en/indices/esg/dow-jones-sustainability-world-index/#.

51 See *RepRisk Research Scope: ESG Issues*, available at https://www.reprisk.com/content/static/reprisk-esg-issues-definitions.pdf. One of RepRisk's designated "social" issues includes "human rights abuses, corporate complicity." RepRisk clarifies: "This issue is linked when a company is accused of committing or being complicit in human rights abuses. This includes, for example, violence against individuals, threat of violence, child and forced labor, human trafficking, organ trafficking, privatization of water sources, *privacy violations*, supporting oppressive regimes or terrorist organizations, trading in 'blood diamonds' or 'bush gold,' etc." (Emphasis added.)

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Moreover, there are signs that interest in ESG investments may be waning, especially in the U.S. As ESG critics become more vocal,[52] some states are withdrawing funds from money managers such as BlackRock because of their decision to invest heavily in companies supporting ESG principles.[53]

According to a 2022 survey of financial planners, the percentage of advisors planning to decrease their allocations to ESG strategies over the next 12 months has more than tripled to 15 percent in 2022—compared to only 4 percent in 2021.[54] Client interest in ESG investing has also waned, with only 31 percent of planners saying they've fielded client questions about ESG investing in the past six months, down from roughly 39 percent in 2020 and 2021.[55] Indeed, Larry Fink, Chairman and CEO of BlackRock, has stopped using the term ESG on grounds that it has become too politicized.[56]

In any event, regardless of whether ESG trends favorably or unfavorably, a holistic data strategy as envisioned by CIPL will endure. That's because it is based on responsible uses of data that have been fully vetted from every angle, thereby limiting risks and maximizing the opportunity for growth.[57]

---

[52] See, e.g., Hans Taparia, *One of the Hottest Trends in the World of Investing Is a Sham*, N.Y. Times, Sept. 29, 2022, available at https://www.nytimes.com/2022/09/29/opinion/esg-investing-responsibility.html. See also, Samuel Gregg, *What's Really at Stake with ESG*, Law & Liberty, Dec. 30, 2022, available at https://lawliberty.org/forum/whats-really-at-stake-with-esg/.

[53] Editorial Board, *Ron DeSantis's war on woke puts BlackRock on the frontline*, Financial Times, Dec. 7, 2022, available at https://www.ft.com/content/ce5bb64d-83dc-4aaa-bcf8-6506732b9b4e.

[54] *2022 Trends in Investing Survey*, conducted by the Journal of Financial Planning and the Financial Planning Association, available at https://www.financialplanningassociation.org/learning/research/2022-trends-in-investing.

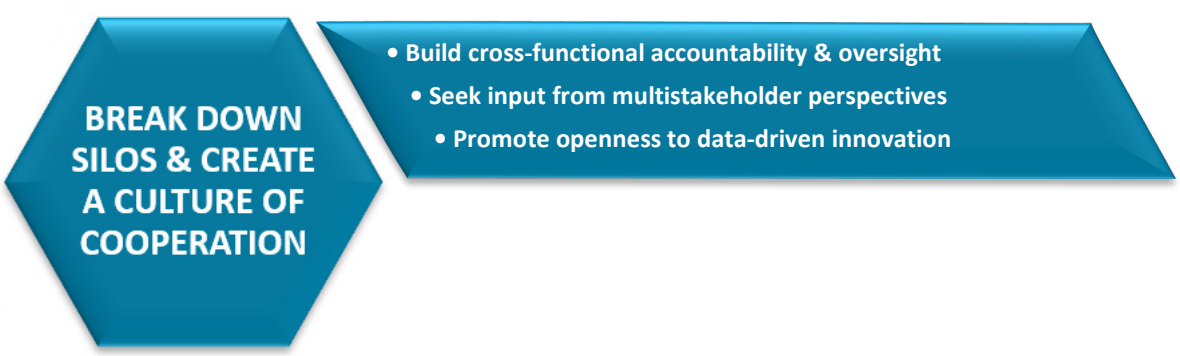
[55] *Id.*

[56] Isla Binne, *BlackRock's Fink says he's stopped using 'weaponised' term ESG*, Reuters, June 26, 2023, available at https://www.reuters.com/business/environment/blackrocks-fink-says-hes-stopped-using-weaponised-term-esg-2023-06-26/.

[57] Regardless of the ebbs and flows in ESG, the UN Sustainable Development Goals (https://sdgs.un.org/goals) continue to be a priority for firms across the globe and are dependent on data to benchmark current realities and to measure progress or shortfalls in relation to those goals.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

STEP THREE



3. BREAK DOWN SILOS AND CREATE A CULTURE OF COOPERATION

A. Build cross-functional accountability and oversight

i. The CIPL Accountability Framework

Those charged with implementing a holistic data strategy would certainly benefit from a review (or re-review) of **CIPL's Accountability Framework**,[58] which assists companies in operationalizing all aspects of data governance.

Seven core elements form CIPL's Accountability Framework: (1) leadership and oversight; (2) risk assessment; (3) policies and procedures; (4) transparency; (5) training and awareness; (6) monitoring and verification; and (7) response and enforcement. *[See Figure 1.]* By encouraging businesses to implement comprehensive privacy and data governance programs based on the CIPL Accountability Wheel or similar frameworks, CIPL has sought to ensure that businesses have processes in place to help them comply with applicable legal requirements and demonstrate good data practices.

Figure 1

[58] See CIPL resources and papers on organizational accountability: https://www.informationpolicycentre.com/organizational-accountability.html.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

For purposes of building **cross-functional accountability and oversight**, CIPL's wheel can serve as a guidepost to help organize a holistic data strategy:

- Leadership & Oversight: Who will head the initiative?
- Risk Assessment: What principal concerns must be addressed?
- Policies & Procedures: What will be the process for vetting proposed uses of data?
- Transparency: Which business units must be included in the conversation?
- Training & Awareness: How will vital communications be filtered throughout the organization?
- Monitoring & Verification: How will the organization ensure that proposed uses of data meet key checkpoints?
- Response & Enforcement: If things go awry, how will they be fixed?

ii. Identify core competencies

Depending on a company's size, an individual or a team can lead the holistic data strategy initiative, but regardless of size, the individual or team should have an understanding of (or at least access to individuals with an understanding of):

- business/revenue generators;
- data architecture and systems;
- applicable privacy and data security laws and regulations;
- compliance obligations;
- IT systems; and
- information security protocols.

In many organizations, the Chief Privacy Officer has a sophisticated understanding of most, if not all, of these areas and could be a suitable lead for a holistic data strategy initiative. In particular:

- data is core to the CPO's initiatives, as all privacy controls are around data;
- the CPO has experience working with other parts of the business to build governance strategies, to ensure privacy-by-design, and to provide guidance on policy issues; and
- the CPO is oftentimes already integrated into many of these business units by virtue of organizational structure.

The holistic data strategy itself should be formalized to ensure that proposed uses of data can be assessed and vetted before a specific proposal is presented to the Board. If the organization has other data-related officers (e.g., CISO, CDO, CTO), the organization should clarify roles and responsibilities of each and determine how they are to relate to each other as well as to the individual or team leading the initiative.

A 2022 study[59] conducted by the European Company Lawyers Association (ECLA) in cooperation with Osborne Clarke suggests that an organization's legal department can be at the heart of data-driven innovation initiatives.

[59] ECLA & Osborne Clarke, *Data-Driven Business Models: The role of legal teams in delivering success*, available at https://www.osborneclarke.com/system/files/documents/22/06/14/Data-driven-business-models-Report-June-2022.pdf.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

However, a 2023 survey of CIPL member companies shows that data governance is, more often than not, an obligation shared among different business units.[60] As one member explained, regulatory issues on data privacy are overseen by the Data Protection Officer within the legal function, while data governance and data security issues are overseen by the Head of Security within the engineering function.

iii. Define appropriate structure

Corporations unaccustomed to viewing data holistically will need to assess whether corporate committees and/or roles already in place have the unique skill set needed to implement a holistic data strategy. A realignment or re-structuring may be required to ensure that all relevant and key stakeholders are engaged, able to contribute, and learn from each other. Alignment with the Board is also important to ensure that implementation and strategy are on the same page.

iv. Recruit cheerleaders

Regardless of the structure agreed upon, organizations should identify "champions" who are not necessarily members of the team leading the initiative but who serve as liaisons with team members and keep departmental employees informed of the team's projects and activities. A virtuous circle of data engagement and sharing is key to ensuring that the data strategy continues to evolve in a manner that continues to be relevant to the organization and that facilitates ongoing change.

B. Seek input from multistakeholder perspectives

i. Culture shift

To the extent an organization is divided into discrete swim lanes—e.g., one for engineering, another for legal, a third for compliance—removal of the lane dividers may arguably be one of the heaviest lifts. Shifts in corporate culture can be threatening to many employees, especially those with long tenures and task-specific priorities. With employee morale and confidence potentially at risk, recognition of past contributions and reassurance of the need for specialized knowledge may be in order. Indeed, corporate messaging that highlights the need to solicit individuals' knowledge and expertise can bolster confidence in the new corporate vision and encourage a willingness to engage in multidisciplinary conversations.

A culture shift can also threaten budget silos, which to some may be as important as employee morale.

While McKinsey has noted the increased presence of chief transformation officers (CTOs) for retail companies,[61] CIPL member companies are taking initiative on their own, with nearly 85% of respondents either strongly agreeing or somewhat agreeing that their organizations are seeking perspectives on proposed data uses from different business units.[62]

ii. Top-down approach

When the call to break down silos originates from top leadership, senior leaders should be the ones conveying the message directly to the rank-and-file, accompanied by an open invitation for

60 See Results of CIPL Member Survey, Appendix, Question 2.

61 *Meet the newest member of the consumer C-suite: The chief transformation officer*, McKinsey Quarterly, Dec. 5, 2022, available at https://www.mckinsey.com/capabilities/transformation/our-insights/meet-the-newest-member-of-the-consumer-csuite-the-chief-transformation-officer.

62 See Results of CIPL Member Survey, Appendix, Question 9.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

volunteers eager to participate in a larger conversation. Increasingly we are seeing the emergence of Data Strategy Officers who are able to convene the relevant stakeholders within an organisation to work together to ensure a coherent data strategy leveraging the expertise and experience across the organisation.

iii. Building up while breaking down

The initiative to break down silos not only supports efforts to embrace a holistic data strategy, but also boosts collaboration and productivity in other areas of the business. Leveraging the skills, expertise, systems, and processes can enable the business to function more effectively and efficiently and can provide new win-win collaboration opportunities between departments and silos not previously thought possible.

C. Promote openness to data-driven innovation

While many corporate leaders recognize that data-driven innovation is fuelling 21st century growth (see Section 1.A.i.), that message may not have yet filtered down the corporate ranks. To get everyone on board and build a culture that embraces data, an organization must educate employees on how and why the company uses data.

What does it take to build a data-driven culture? An article published by Harvard Business Review answers that question.[63] The authors, two employees at Kuwait's Gulf Bank, sought to launch a digital transformation of the bank's operations, focussing principally on data quality. To change the culture and encourage a digital mindset, they wanted all 1800 bank employees to understand two things: "that everyone needs data to do their job (i.e., they are data customers), and that they also create data used downstream (i.e., they are data creators)."[64] Among the ideas used to advance that initiative was the creation of a "data ambassadors" program (similar to the "cheerleaders" idea mentioned above), and a "Data 101 program," which explained employees' dual roles as data creators and customers. The result?

> As we expected, ambassadors and others across the bank began working together, making measurements, targeting data cleanups, and eliminating root causes of error. Then, somewhat organically, ambassadors and regular employees began using methods and tools provided in the training in new ways, to innovate on their own. For example, two ambassadors joined forces to improve anti-money laundering models, enhancing the customer experience in the branch, while simultaneously reducing risk and operational expense.[65]

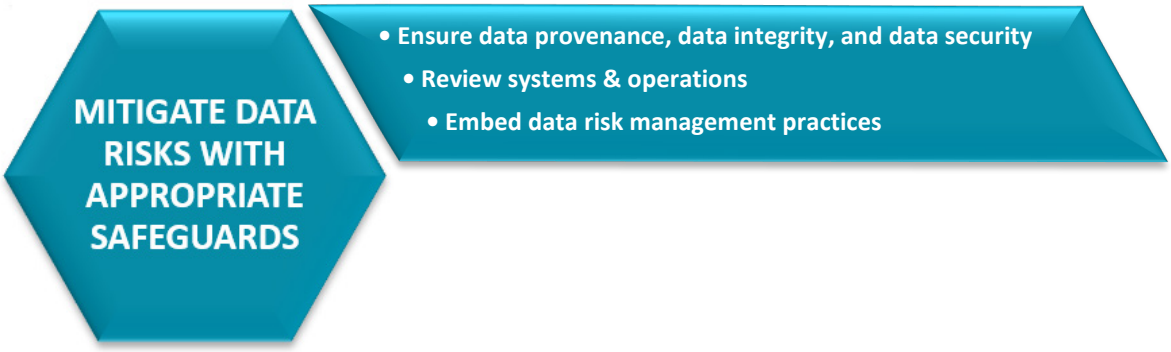
63 Mai B. AlOwaish and Thomas C. Redman, *What Does It Actually Take to Build a Data-Driven Culture?* Harvard Business Review, May 23, 2023, available at https://hbr.org/2023/05/what-does-it-actually-take-to-build-a-data-driven-culture.

64 *Id.*

65 *Id.*

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

STEP FOUR



4. MITIGATE DATA RISKS WITH APPROPRIATE SAFEGUARDS

A. Ensure data provenance, data integrity, and data security

Data provenance, which refers to a documented trail that accounts for the history of a piece of data, is essential to a holistic data strategy. Indeed, data integrity and data lifecycle management are critical to any business use, so it is important to know the origin of any given data set. How and when was it compiled and by whom? Has it been modified or filtered in any way? Has any processing taken place that can compromise its accuracy or completeness? Questions such as these are fundamental to ensure that business decisions are based on reliable data. In the AI context, the sources and accuracy of data are particularly significant to avoid bias and discrimination. Data lifecycle management also addresses how data is used and by whom, where it is shared and stored, and when it is updated and deleted.

Data security considerations are closely tied to data integrity concerns, so those implementing a holistic data strategy will need to assess the safeguards currently in place, and whether those safeguards need supplementation or fine-tuning.

Moreover, as digital threats continue to rise, a holistic data strategy should consider not only internal security measures to reduce the risk of attacks, but also insurance coverage to protect against losses in the event of an attack. In recent years, cyber insurance costs have soared, prompting some to predict that cyberattacks will become "uninsurable."[66] Others, however, are more sanguine, noting that the cyber insurance industry "is young enough to claim adolescence as the reason for frequent rapid changes in the market."[67]

Still, insurance coverage is vital. The SEC's new Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure[68] (discussed infra) emphasize that companies have significant

[66] Ian Smith, *Cyber attacks set to become 'uninsurable', says Zurich chief*, Financial Times, Dec. 26, 2022, available at https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d.

[67] Oliver Brew, *Cyber Insurance Themes to Look Out for in 2023*, Insurance Journal, (Jan. 3, 2023), available at https://www.insurancejournal.com/news/national/2023/01/03/701440.htm.

[68] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Final Rule), 88 FR 51896 (Aug. 4, 2023), available at https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

exposure from cyber incidents. While cyber and D&O policies can help mitigate these risks, companies should carefully evaluate their policies to determine what coverage—and gaps in coverage—exist.[69]

B. Review systems and operations

Organizations should anticipate that security incidents and breaches will occur. A holistic data strategy should include a re-review of the company's incident response plan to ensure that any proposed uses of data would be addressed under the plan. Those charged with implementing the strategy should also reach out to members of the incident response team to inform them of the proposed use and give them time to make adjustments to the plan or raise concerns about a potential breach involving the underlying data.

While internal threats still rate highly for companies, businesses should take a holistic view of internal and external data dependencies in order to address supply chain vulnerabilities, nation state threats, ransomware and malware attacks, and business email compromise.[70]

To the extent pertinent data is already subject to a retention or deletion protocol, a holistic data strategy must ascertain whether exceptions or modifications will need to be made.

C. Embed data risk management practices

Risk management has long played an important role in data protection, and its role is no less important in the context of a holistic data strategy. As noted by CIPL in a 2016 White Paper, "[risk management] facilitates thoughtful, informed decision making by organizations by requiring them to explicitly consider both the harms and benefits not only to the organizations but also to the data subjects, and by focusing increasingly scarce resources of both organizations and government regulators where they are needed most."[71]

Unfortunately, more than eight years after the publication of that paper, stakeholders are still awaiting consensus on one of the paper's key recommendations: articulating a clear understanding of the harms that risk management is intended to identify and mitigate. While there has been some progress in elaborating typologies of harm[72] and most stakeholders are no longer "equating harm to data collection without proper notice and consent,"[73] many are still equating harm to the type of data at issue (i.e., so-called "sensitive data").

As noted by CIPL in a recent response to a consultation, risk management "does not address whether **certain types of data should be used generally or at all**, but rather whether **the data can be used responsibly and with appropriately tailored protections in a specific context and for a**

---

69 Reducing Risks from Cyber Incidents with Cyber and D&O Insurance, Privacy & Information Security Law Blog, Hunton Andrews Kurth (Aug. 10, 2023), available at https://www.huntonprivacyblog.com/2023/08/10/reducing-risks-from-cyber-incidents-with-cyber-and-do-insurance/.

70 John Wilson, Cybersecurity Threats In 2023: An Expert's Top 5 Predictions, Forbes Advisor (Dec. 19, 2022), available at https://www.forbes.com/advisor/personal-finance/cybersecurity-threats-for-2023/.

71 CIPL Discussion Draft: The Role of Risk Management, Feb 16, 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf.

72 For example, see Danielle Keats Citron and Daniel J. Solove, *Privacy Harms*, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222.

73 *Supra*, note 71, p. 8.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

specific purpose."[74] Thus, when embedding data risk management practices for a holistic data strategy, companies should adopt organizational accountability measures that include **contextual risk assessments** to help companies:

- evaluate the sensitivity of data and data uses in context, along with the attendant level of risk;
- identify high-risk processing and tailor compliance and mitigation measures to such risk;
- identify legitimate and beneficial uses of data;
- evaluate individual, organizational, and societal benefits of data uses; and
- document their risk assessments and compliance and mitigation measures and be able to explain their processing decisions under relevant legal standards.[75]

[74] CIPL Response to NTIA Privacy, Equity, and Civil Rights Request for Comment, March 6, 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_ntia_privacy_equity_and_civil_rights_request_for_comment__6_march_2023_.pdf (emphasis in original).

[75] *Id.*

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

STEP FIVE

5. HARMONIZE DATA-RELATED COMPLIANCE OBLIGATIONS

A. Understand data protection laws and use of PETs

As stated earlier, a holistic data strategy is not and should not be limited to personal information. However, to the extent that personal data will be processed, those charged with implementing the strategy should have a solid understanding of data protection laws and regulations that pertain to such data, including the rights of individuals with respect to the processing of their data. They should also be familiar with Privacy Enhancing Technologies (PETs) and Privacy Preserving Technologies (PPTs) to help manage the risks associated with the processing of personal data.[76]

Generally speaking, organizations should ensure that the collection and use of data is fair and lawful. These standards, often referred to as "**data protection principles**," tend to be similar in data protection frameworks across the globe. Compliance with these principles enables organizations to foster trust both with the individuals whose data is being processed and with the regulators who enforce the laws.

B. Address multi-jurisdictional compliance challenges

Whether a given data set constitutes "personal data" will vary from jurisdiction to jurisdiction, so it is important to understand how the data will potentially flow and which jurisdictions' laws may apply. Equally important is the knowledge of exceptions and exemptions to those laws—such as when personal data is rendered anonymous—along with the knowledge of technical measures used to anonymize or otherwise modify the obligations of a given law.

Significantly, if proposed data uses involve the transfer of data across borders, the company will need to assess which data transfer mechanism would be most appropriate under the circumstances.

---

[76] See CIPL White Paper, *Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age*, Dec. 12, 2013, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

C. Resolve cross-disciplinary legal obligations

While a holistic data strategy encourages organizations to view data beyond the lens of compliance, that doesn't lessen the importance of compliance obligations or demand that they be ignored. Instead, a holistic data strategy examines and recognizes compliance issues along with other costs of doing business. Input from the compliance team is essential to determine whether a new data use requires additional compliance efforts or whether it can be incorporated easily into an existing framework.

Ideally, persons responsible for implementing the strategy would already have access to members of the legal and IT departments to address data protection and data security issues, but the potential scope of inquiry may extend beyond the parameters of those laws. Antitrust and competition concerns may also need to be addressed, as regulators are increasingly viewing data issues through both a privacy and antitrust lens.[77] In the case of generative AI, the vetting process may extend to intellectual property, anti-discrimination, and consumer protection laws. And, to complicate matters even more, the vetting process should include not only existing laws and regulations, but also those on the horizon.

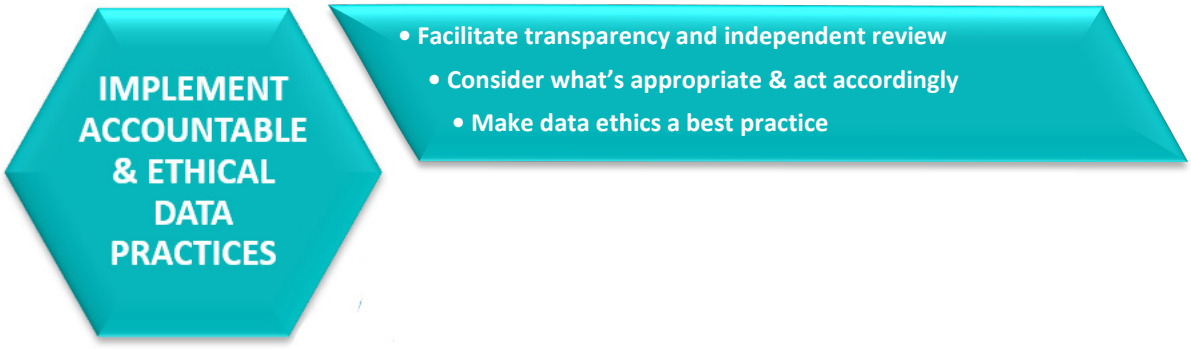
To the extent the law is unclear with regard to a proposed use, the organization should consider reaching out to **regulators** for guidance, thereby demonstrating the organization's willingness to do the right thing. CIPL encourages organizations to foster cooperative relationships with regulators, and, where novel uses are proposed, supports the use of regulatory sandboxes, policy prototyping, and other innovative regulatory methods to address compliance challenges associated with new technologies and business practices.

In addition to soliciting legal guidance on the specific areas of law addressed above, those implementing a holistic data strategy should touch base with the organization's **General Counsel** or other legal officer to identify non-privacy issues that may factor into an assessment (such as pre-existing contractual obligations, potential mergers or acquisitions, tax liabilities, vendor management concerns, intellectual property licensing obligations and restrictions, inter-group processing agreements and risk assessments, ethical issues etc.).

[77] Paulette Rodríguez López, *Increased Enforcement Shows Firms Need to Plug Antitrust and Privacy Law Requirements Into Their Digital Algorithms*, June 9, 2022, available at https://constantinecannon.com/antitrust-group/antitrust-today-blog/increased-enforcement-shows-firms-need-to-plug-antitrust-and-privacy-law-requirements-into-their-digital-algorithms/. See also, Section 1D, *supra*.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

STEP SIX



6. IMPLEMENT ACCOUNTABLE AND ETHICAL DATA PRACTICES

A. Facilitate transparency and independent review

Transparency, along with monitoring and verification, comprise two of the seven elements in CIPL's Accountability Framework (discussed *supra*). Without minimizing the importance of the other five elements, these two are arguably the most pertinent in the context of data ethics, for they deal with openness and candor. Specifically, they require companies to:

- provide transparency to all stakeholders internally and externally, and
- monitor and verify the implementation and effectiveness of the program and internal compliance.

Of course, these elements are closely related to the Board's mission to build trust and reputational integrity (discussed *supra*). Transparency, in particular, is critical for generating trust from both individuals and regulators:

> By effectively informing individuals about the protection and use of their personal data, including benefits of data processing, and by addressing the concerns of regulators, transparency will have the effect of raising the level of digital education, broadening individuals' expectations, increasing their acceptance of and support for certain data uses, and generally deepening individuals' and regulator trust.[78]

Accordingly, fulfilment of the Board's mission to build trust will drive the operationalization of ethical practices.

[78] CIPL Comments on the FTC's ANPR on Commercial Surveillance and Data Security, Nov. 21, 2022, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_ftc%E2%80%99s_anpr_on_commercial_surveillance_and_data_security__21_nov_2022_.pdf.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

While internal audits certainly play a role in responsible data practices, external audits can provide more robust and neutral views on particularly difficult ethical and compliance issues and may therefore be viewed as more credible by the public.[79]

Relatedly, many organizations have established **ethics advisory boards** to provide valuable perspective on unsettled practices. It is no longer sufficient for the Board and the C-suite to ensure mere compliance with legal and regulatory obligations; an ethical approach is expected by employees, customers, stakeholders, and regulators. Understanding and demonstrating an ethical approach is an essential element of every business's data strategy. Indeed, 75% of respondents to CIPL's member survey either strongly agree or somewhat agree that their organizations have or are planning to have a data ethics committee.[80]

In the AI context, CIPL has noted that ethics bodies should consist of individuals with a range of diverse life experiences, multidisciplinary skill sets, and, if the body is internal, different roles within the organization. CIPL has also noted the importance of establishing clear procedures for presenting matters to the ethics body, including cadences for ongoing review of research and business activities as well as emergency escalations for time-sensitive decisions.[81]

B. Consider what's appropriate and act accordingly

According to Harvard Professor Dustin Tingley, data ethics asks: Is this the right thing to do? Can we do better?[82]

An organization must be thoughtful about risks to its business and the individuals it affects. It must not only establish controls and incentives that drive responsible and ethical behavior, but also demonstrate that this is the case. Accountability requires organizations to show that they are fully cognizant and in control of their impact on people and the environments in which they operate.[83] As noted above, demonstrability is a key feature of privacy maturity models, like CIPL's Accountability Framework. Demonstrability enables corporate leaders to communicate the benefits of a holistic data strategy to core stakeholders, such as the Board, shareholders, customers, and regulators.[84]

C. Make data ethics a best practice

Over the past several years, there has been an increased focus on creating accountable and ethical frameworks for the use of advanced technology such as AI, and addressing difficult issues like bias, non-discrimination, and forms of redress. There are growing expectations that organizations should implement accountability and ethical data principles in the development and use of new technologies.

Oftentimes, ethical considerations can be implemented as part of an organization's accountability obligations, but a common pitfall for business leaders is thinking that legal and compliance have data

---

79 CIPL Response to NTIA Request for Comment on AI Accountability Policy, June 12, 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_ntia_ai_accountability_policy_june2023.pdf.

80 See Results of CIPL Member Survey, Appendix, Question 11.

81 CIPL Response to NTIA Request for Comment on AI Accountability Policy, *supra*, note 79. CIPL's forthcoming report on accountable AI governance practices will discuss the use of ethics advisory boards in greater detail.

82 Catherine Cote, *5 Principles of Data Ethics for Business*, Harvard Business School Online's Business Insights Blog, Mar 16, 2021, available at https://online.hbs.edu/blog/post/data-ethics.

83 See Rodríguez López*, supra*, note 77.

84 Compare Cisco-CIPL Report, *supra*, note 17.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

ethics covered. Indeed, one way to avoid that pitfall is to recognize that data ethics are a shared responsibility across an organization, and not the province of any single team.[85]

Ethics is largely defined by expectations: the expectations of consumers, shareholders, regulators, and society at large. Each stakeholder's expectation regarding a specific use may be different, but in the end, all must agree that the use is acceptable, i.e., that the organization earns their trust.[86]

CONCLUSION

CIPL's roadmap for a holistic data strategy hopes to embolden businesses not already accustomed to leveraging data insights to view data beyond the lens of privacy compliance. At the direction of the Board and with the support of executive leadership, formerly siloed corporate units can share institutional knowledge and unlock the hidden value of data for legitimate, innovative, and beneficial business purposes, including the responsible development and use of AI. Chief Privacy Officers, who are already equipped with knowledge of the risks inherent in uses of data, are uniquely positioned to lead a holistic strategy, but the corporate Board must take the first step in recognizing the potential of data-driven innovation.

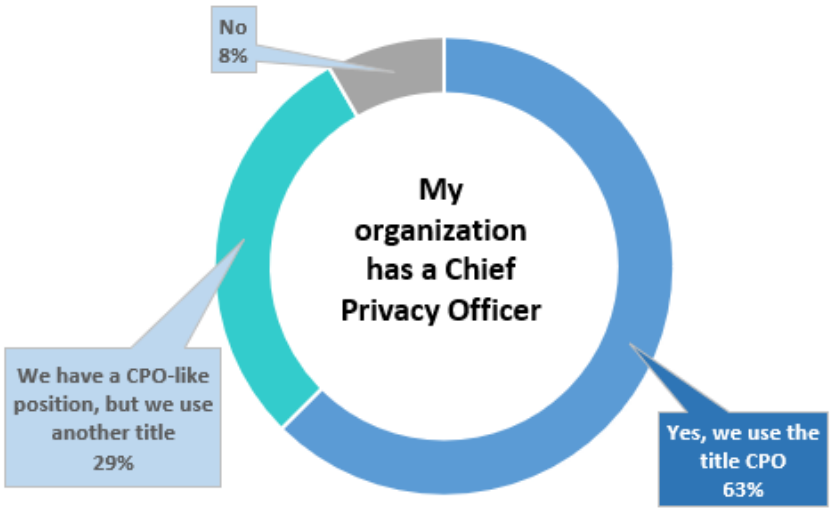
85 Alex Edquist et al., *Data ethics: What it means and what it takes*, McKinsey, Sept. 23, 2022, available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes.

86 See Section 2.B., *infra*.

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

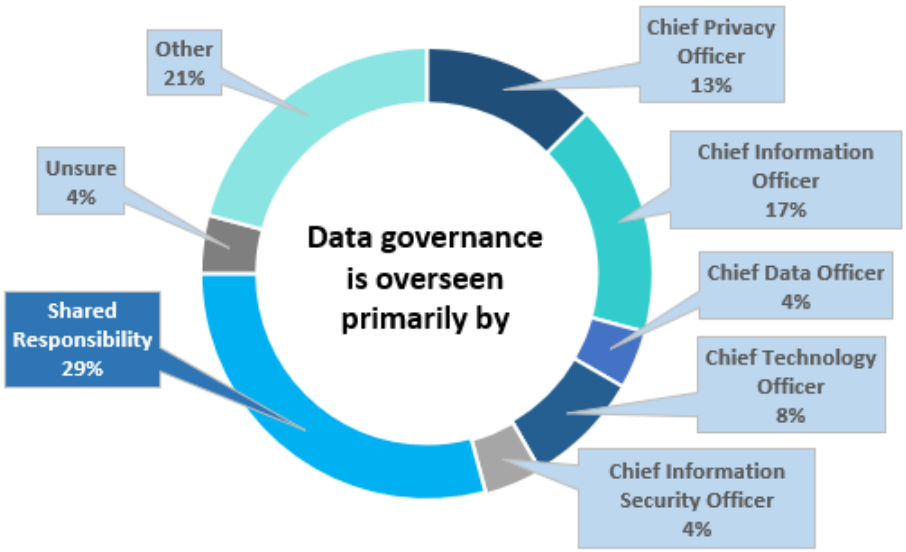
APPENDIX:
CIPL MEMBER SURVEY 2023

1. My organization has a Chief Privacy Officer:



Source: CIPL Member Survey 2023

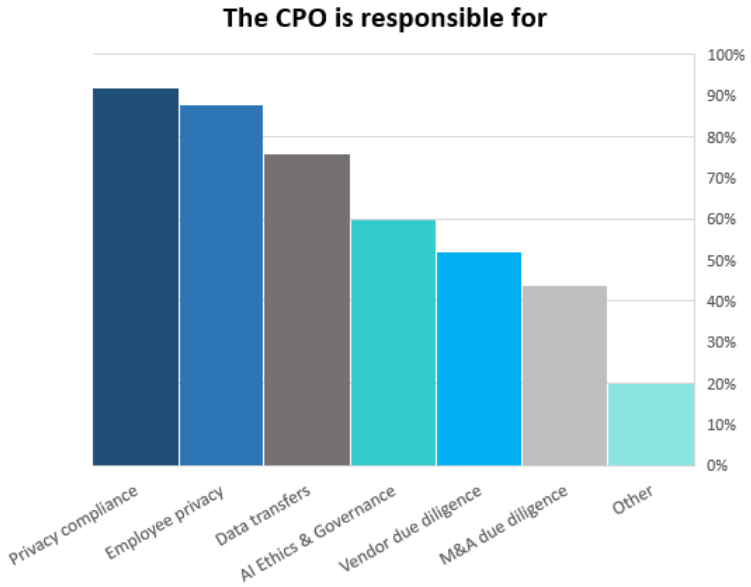
2. In my organization, data governance issues are overseen primarily by:



Source: CIPL Member Survey 2023

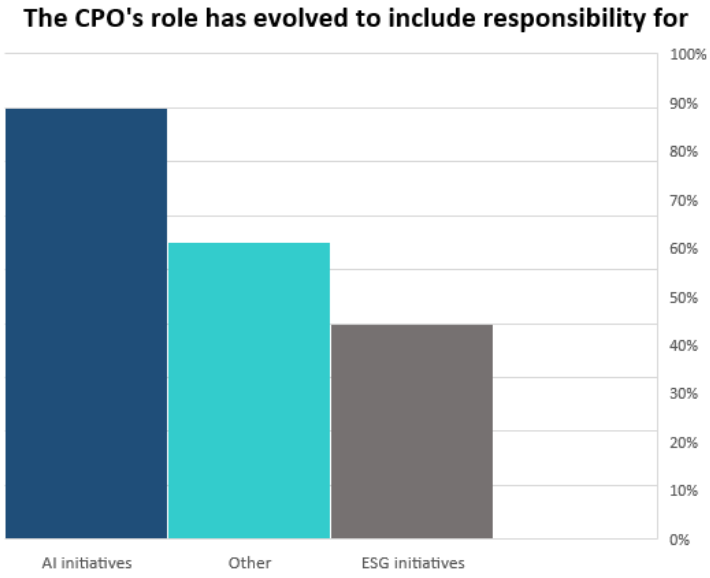
Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

3. In my organization, the Chief Privacy Officer [or the person identified in response to Q1] is responsible for (check all that apply):



Source: CIPL Member Survey 2023

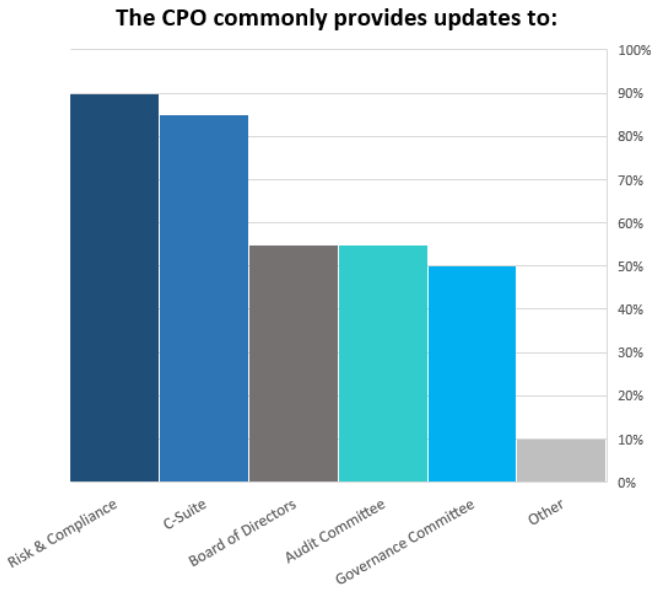
4. In my organization, the Chief Privacy Officer's role [or the role identified in response to Q1] has evolved to include responsibility for (check all that apply):



Source: CIPL Member Survey 2023

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

5. In my organization, the Chief Privacy Officer [or the person identified in response to Q1] commonly provides updates to (check all that apply):



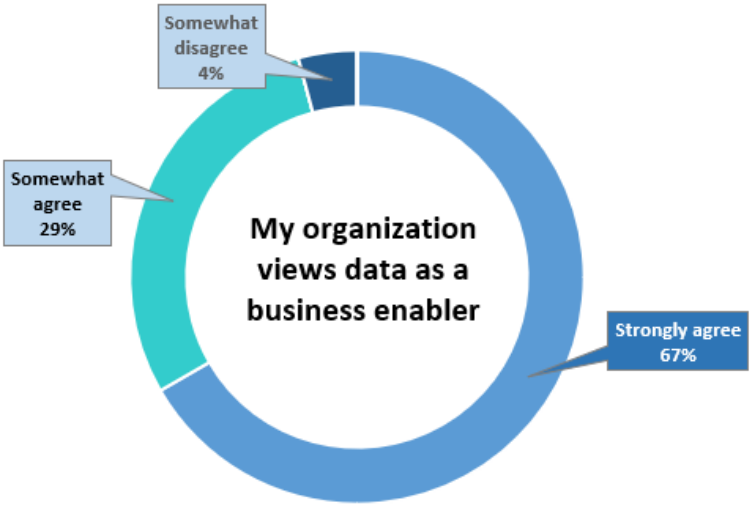
Source: CIPL Member Survey 2023

6. My organization primarily views data governance as a matter of risk & compliance.

Source: CIPL Member Survey 2023

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

7. My organization views (or is starting to view) data as a business enabler.



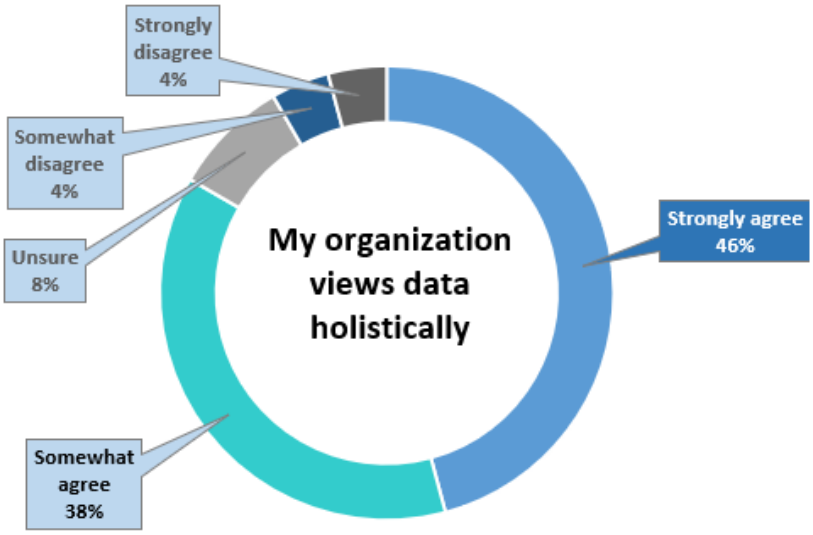
Source: CIPL Member Survey 2023

8. My organization views (or is starting to view) data governance issues through the lens of ESG.

Source: CIPL Member Survey 2023

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

9. My organization views (or is starting to view) data holistically, i.e., seeking perspectives on proposed data uses from different business units, such as technology, information security, legal, compliance, product development, and others.



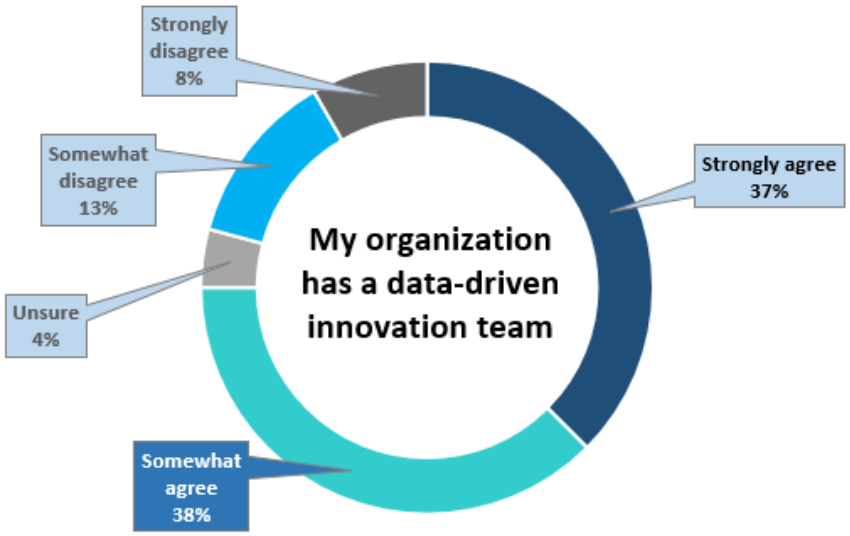
Source: CIPL Member Survey 2023

10. My organization has (or is planning to have) a data-driven innovation center or team.

Source: CIPL Member Survey 2023

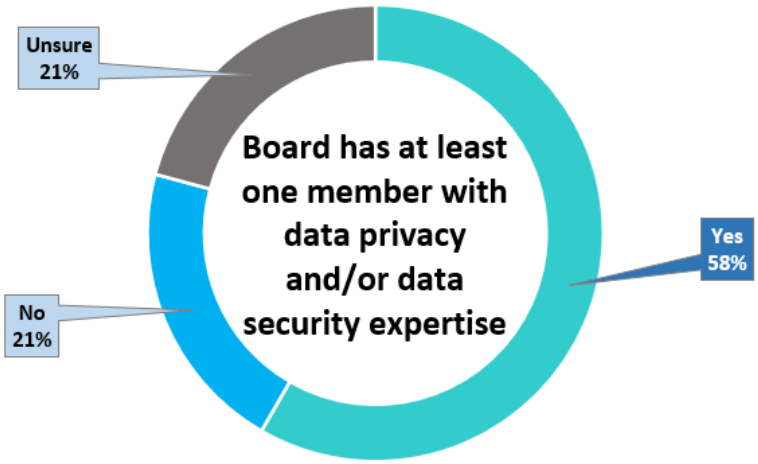
Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

11. My organization has (or is planning to have) a data ethics committee.



Source: CIPL Member Survey 2023

12. My organization's Board of Directors includes at least one member with experience or expertise in data privacy and/or data security issues.



Source: CIPL Member Survey 2023

Copyright © 2024 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.