Embedding
PROJECT

GOVERNANCE AND ETHICS

Data Oversight

A GETTING STARTED GUIDE

Brandon Toews

Data Oversight

A GETTING STARTED GUIDE

Prepared by Brandon Toews.

Brandon Toews. *Data Oversight: A Getting Started Guide.* (Embedding Project, 2026).
DOI: 10.6084/m9.figshare.33200967

CONTENTS

ABOUT THIS SERIES

This guide is part of our series of Getting Started Guides that supports your company to develop an embedded sustainability strategy. Each guide tackles a specific sustainability sub-issue and explores what your company needs to do to support the resilience of the environmental and social systems around you.

In each guide, we address relevant trends, system thresholds, key concepts, key actors, and key resources. We also offer guidance on how to address the impacts of decisions and activities in your operations and value chains as well as developing credible goals and outlining key corporate actions and internal targets that can help to provide clarity on the work ahead.

We recommend you read the first guide in the series, Getting Started Guides: An Introduction, which explains our overall approach and the value of setting a clear strategy anchored in your company's most material issues. It also explains how you can leverage process-based interim targets to clearly outline and track the specific actions that your company needs to take to achieve its high-level goals.

A complete list of focus areas and sub-issues can be found in our guide Scan: A Comprehensive List of Sustainability Issues for Companies.

This guidebook addresses **Data Oversight**, which is part of the broader sustainability issue of *Governance and Ethics*.

1 SETTING THE STAGE – THE ERA OF BIG DATA

Data is a vital prerequisite for business. Data informs business decisions and strategy, drives growth, and powers innovation, and none of that can happen without good data oversight. Good data oversight can help organisations to procure, manage, and protect large amounts of data by improving data collection, ensuring data quality, reducing data siloes, and upholding data policies and commitments, among other functions.

Data oversight is rapidly evolving. Significant trends are reshaping our understanding – and the future – of data oversight. As the volume and vulnerability of data grows, organisations need to (re)consider their data oversight policies, practices, processes, architecture, roles, and responsibilities to effectively scale their business intelligence efforts.

The global regulatory landscape around data is rapidly evolving, with new laws and amendments that focus on how businesses collect, store, manage, and use personal data. There is a growing number of data privacy and protection regulations and laws, such as those mandating that data be stored domestically, and measures that condition the movement of data across international borders.

Key among them was the EU's General Data Protection Regulation (GDPR), which came into effect in 2018. This law protects the personal data of EU residents, and it requires organisations – including those outside the EU – to comply with certain data protection standards when handling the personal data of EU residents. Since then, laws similar to – and influenced by – the GDPR have been adopted around the globe, including in Canada, Brazil, South Africa, the USA, and more.

Data privacy legislation is gaining momentum across the US, with nearly two dozen states passing comprehensive data privacy laws. Notably, the California Privacy Rights Act (CPRA) came into full effect in 2024, enforcing stronger consumer rights, data minimisation, and requiring businesses to provide clearer explanations about how they process personal data. The GDPR has also influenced information security standards used by businesses, such as the Payment Card Industry Security Standards Council.

The consequences of non-compliance with data protection laws have also become more severe, with growing fines and potential for reputational damage.

As a result of these regulations, a key challenge facing businesses is data sovereignty. As data resides in jurisdictions with differing regulatory requirements, businesses must ensure that their data governance policies adhere to the specific rules of the regions in which they operate. This has led to the rise of geo-fencing solutions that enable companies to restrict data flows across borders, ensuring compliance with regulations.

There is also growing scrutiny of data oversight in relation to human rights and government efforts to undermine them. There is growing concern that companies are complying with laws that aim to undermine citizens' rights. This includes increasing pressure on companies from authoritarian governments to hand over users' data, facilitate mass surveillance, censor and moderate content, and manipulate online discussions.

For example, large US-based tech firms have been identified by the UN Office of the High Commissioner of Human Rights as being complicit in aiding an "economy of genocide." Alphabet, Amazon, and Microsoft have been criticised for providing Israel with virtually government-wide access to their cloud and AI technologies, thereby enhancing data processing and surveillance capacities and aiding Israel in the displacement of Palestinians and its genocidal war on Gaza. Other large tech firms – such as Meta, Youtube, and X – have been identified as complicit in systemic mass censorship of Israeli violence towards Palestinians across major social media platforms.

More recently, these same large tech firms – as well as other social media companies – are facing growing pressure from the US government to hand over user data on accounts that track or comment on the actions of the executive branch, such as violence and murders carried out by Immigrations and Customs Enforcement (ICE). The Department of Homeland Security has significantly expanded its efforts to subpoena information that identifies Americans who oppose ICE, including legal requests for names, email addresses, telephone numbers, and other identifying data.

There are also nascent concerns about emergent neurotechnologies and how they could be exploited. There are growing concerns that both medical and non-medical devices – including both wearables and those designed to be implanted into the body – may enhance inequalities, such as within educational settings. There are also concerns that information such as eye movement and tone of voice could be used to infer neural data, such as someone's state of mind or brain activity, and that this data could be exploited to manipulate or influence decisions, such as those related to commercial advertisements or political messaging. Ethical principles for governing neurotechnologies are being explored and developed to better ensure that users are protected from technology misuse that could infringe upon their autonomy and freedom of thought, among other human rights.

Meanwhile, artificial intelligence technology is advancing rapidly. There has been a recent surge in companies developing and incorporating AI and machine learning into data governance, management, and analysis, with a growing number of organisations working to create structures and processes and redesign workflows to better capture the value of these new technologies. Particularly prominent is the advent of increasingly autonomous systems, such as agentic AI, which can plan, execute, and manage operational tasks with little or no human oversight.

The capabilities of AI are broad, and so too are use cases. Businesses are increasingly using AI for content generation; sales forecasting; price optimisation; quality control and assurance; targeted marketing; customer support; as internal knowledge assistants; and more. Sustainability professionals and teams are also rapidly adopting and integrating the technology. The vast majority of sustainability professionals are using AI in some capacity in their roles, such as for workflow support; supporting ESG data quality checks and reconciliation; extracting and assessing data across filings and systems; measuring, monitoring, and forecasting impacts; carbon accounting; risk analysis and scenario planning; and for supply chain optimisation.

Accompanying the proliferation of these new technologies are a range of ethical concerns. These technologies have significant implications for industry, and especially for the global workforce. Although recent reporting posits that AI will create more jobs than it displaces, at least in the short term, there are also signs that new technologies will significantly reshape the world of work, with some estimates suggesting that half of all jobs globally could be automated within twenty years.

There are also growing concerns around digital amplification, with AI enhancing the reach and influence of digital content and raising ethical concerns around transparency, fairness, and the potential for misinformation and disinformation.

Algorithmic bias carries the risk of systematic discrimination, and – in the context of industry – prejudiced data threatens to produce unfair outcomes, such as unfairly prioritising certain candidates during recruitment.

The scope, scale, and sophistication of cybersecurity threats is rapidly growing, due in large part to bad actors having easy access to formidable AI tools. The risk of phishing attacks, malware and ransomware, data breaches, and other cybersecurity threats is growing, and can lead to financial losses (including fines and litigation), the loss of sensitive data and intellectual property, and damage to reputation. Publicly-traded companies face growing expectations to provide more detailed disclosures and filings regarding their cybersecurity practices, including their cybersecurity strategy, risk management process, and the board's role in oversight.

Despite the broad and growing range of social and environmental impacts related to implementation, and despite increasing scepticism and mistrust of AI, rising costs, and the risk of amplifying the scale, scope, and consequences of bad judgement, adoption of AI technologies is rapidly growing.

There is tremendous pressure on firms to integrate and automate, and all while navigating the nascent field of AI and an evolving set of guiding principles and ethics. We are already seeing the development and introduction of AI-related regulations, such as the EU's AI Act, which is intended to ensure that AI systems are safe, fair, and respect peoples' rights.

It is increasingly clear that businesses must prioritise the handling of sustainability data and invest in relevant data systems, such as sustainability data dashboards. Yet, although sustainability data has emerged as financially relevant and a key contributor to the long-term decision-making, stability, and success of businesses, many companies have not invested in the necessary data infrastructure, instead relying on decentralised or parallel systems rather than ones where sustainability data is embedded.

Companies need to understand that data is a mission-critical asset and exercise appropriate oversight. This means pursuing effective data governance and stewardship; understanding your data use, risks, and impacts; addressing vulnerabilities; supporting good data oversight throughout your operations and value chain; and setting appropriate expectations for reporting and disclosure.

Note: Sustainability issues are generally systemic issues, because they are deeply interconnected and rooted in complex environmental, social, and economic systems. In these guides, a system threshold is defined as the point at which the resilience of an environmental, social, or economic system becomes compromised. This occurs when the total impacts imposed on the system exceed its capacity to assimilate those impacts.

SYSTEM THRESHOLD

The importance of data oversight goes beyond material risks to your organisation. Data privacy is a fundamental human right, and companies have a key role to play in upholding it – beyond just complying with the evolving set of global and regional regulations.

Data oversight matters because it ensures the responsible and ethical use of data. Companies have a responsibility to collect, store, and use the least necessary amount of data, and to ensure that the data they collect is protected from unauthorised access. The mismanagement of data contributes to a broad and growing range of acute and chronic impacts – on individuals, organisations, and societies at large. Breaching, harvesting, and leaking or selling personally identifiable information and other sensitive data is contributing to fraud, identity theft, extortion, and more. Misuse of data and other malicious cyber activities is also contributing to broad systemic issues such as interference in democratic processes and elections and the spread of misinformation and disinformation.

The right to privacy is recognised in Article 12 of the Universal Declaration of Human Rights; Article 17 of the International Covenant on Civil and Political Rights; and resolution 68/167 on the right to privacy in the digital age, wherein the United Nations General Assembly affirmed that the rights people have offline must also be protected online, including the right to privacy. More recently, in response to a Human Rights Council resolution, the Office of the United Nations High Commissioner for Human Rights (OHCHR) is in the process of preparing a report on challenges and risks with regard to discrimination and unequal enjoyment of the right to privacy associated with the collection and processing of data in the digital age, as well as the identification and clarification of related human rights principles, safeguards, and best practices.

The right to privacy is further enshrined in international and regional human rights instruments, such as Article 8 of the European Convention of Human Rights and Article 7 of the European Charter of Fundamental Rights. Beyond these thresholds, the OECD Privacy Guidelines articulate data protection principles for collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

KEY TOPICS WITHIN DATA OVERSIGHT:

- Data collection (data minimisation; ensuring data collection is fit for purpose)
- Data ownership and sovereignty
- Data governance
- Records and data management (cybersecurity and data protection; data at rest encryption)
- Prevention of data misuse or unauthorised use
- Responsible management of personally identifiable information
- Data use (data comparability; fair and lawful data processing; ethical implications of machine learning; responsible use of artificial intelligence)
- Responsible data retention and disposal
- Storage limitations

2 KEY CONCEPTS

The absence of consistent definitions for key concepts is a challenge when discussing data oversight and related topics. There are many interrelated concepts and considerable variation in how these concepts are defined, arranged, prioritised, and understood in relation to one another. In the course of our research, we found many competing definitions for key concepts articulated by governments and intergovernmental organisations, nongovernmental organisations, individual companies and industry groups, and thought leaders.

From among these sources, we found that the United Nations Economic Commission for Europe (UNECE) and the Data Management Association (DAMA) provide some of the more cogent and consistent definitions. To advance data stewardship and governance, the United Nations Economic Commission for Europe has sourced and cited definitions from a range of experts from across the public and private sectors and academia with the aim of developing a unified understanding and definition of key concepts (including from DAMA). From among the key concepts and definitions they have collected, it is particularly important that you first understand **data governance, data stewardship, data ownership, data sovereignty**, and **master data**.

Data governance can be defined as the exercise of authority, control, and shared decision-making (such as planning, monitoring, and enforcement) over the management of data assets. It can also be defined as a system of decision rights and accountabilities for the management of the availability, usability, integrity, and security of data and information, and the regulations, policies, and frameworks that provide enforcement. Most simply, however, it can be understood as the "rulebook" that sets out the policies, procedures, and roles that develop, oversee, and coordinate how data is managed across the organisation – including how data is collected, organised, stored, accessed, used, transformed, shared, protected, monitored, and more. It is everything you do to ensure data assets are secure, private, accurate, available, and usable, including all the actions people must take, the processes they must follow, and the technology that supports them throughout the data life cycle.

There are many frameworks and models for effective data governance, and they can vary widely in their structure and presentation. However, a common theme is that data governance provides the strategic oversight and policy framework that ensures an organisation's data is reliable, consistent, and compliant with regulations.

Data governance sets the "rules" and provides the strategic framework, authorisation, and oversight for data stewardship, which implements and enforces these rules. **Data stewardship** is a collection of data management practices designed to help ensure that data is accurate, consistent, up-to-date, and accessed and used appropriately across the organisation, and can be thought of as "data governance in action." Common data management activities include data collection (including data minimisation and ensuring data is fit-for-purpose), verification, encryption, storage, organisation, and analysis.

Complementary to data governance and stewardship is data ownership and data sovereignty.

Data ownership generally refers to your organisation's responsibility and accountability for data, including for accuracy, security, and compliance. It can also refer to the right to possess, use, and dispose of data. **Data sovereignty** is the concept that data belongs to – and should be subject to the laws and regulations of – the nation or region where it is generated, collected, stored, processed, and/or distributed. This ensures that data is controlled by pertinent entities – such as individuals, organisations, or communities – and that they have the authority to determine how their data is used. This means that the government of that nation has the authority to control access to the data and can require companies to store it within the nation's borders (this requirement is known as **data localisation**). In an Indigenous context, Indigenous data sovereignty describes the fundamental rights of Indigenous Peoples to control, access, interpret, manage, and collectively own their data.

These aspects of data oversight are deeply interconnected, and effective oversight requires them to operate in harmony. Data governance provides the framework, data stewardship provides the execution, data ownership provides the accountability, and data sovereignty ensures that organisations, governments, and individuals have control over their data. Combined, they ensure that data is accurate, secure, effective, and compliant with regulations.

Master data is the core, authoritative data that your organisation collects and uses to measure, manage, and disclose performance consistently across the company. It provides a single "source of truth" for those referencing and leveraging data. Increasingly, companies are identifying sustainability-related master data, which can include data related to the environmental, social, and governance aspects of products, materials, processes, suppliers, employees, and more. Some common sustainability master data elements include greenhouse gas emissions factors and data, water consumption, hazardous substance information, ecosystem health data, human rights information, compensation ratios, grievance data, and sustainability-related training completion. Identifying sustainability-related master data helps to prevent data conflicts and to ensure accurate and consistent reporting. It also helps with better decision-making, regulatory compliance, governance controls, and traceability.

As AI use increases, it is crucial to recognise the integral link to comprehensive master data. AI models are only as good as the underlying data; well-governed sustainability master data improves the quality of insights.

It is also important to understand **cybersecurity, data protection, data privacy**, and **data security**.

At a high level, **cybersecurity** refers to all the aspects of protecting an organisation and its employees and assets (such as computer systems, networks, and data) against cyber threats, including unauthorised access, misuse, theft, and/or damage.

Data privacy and data security address different yet interrelated aspects of data protection.

Data privacy, often referred to as information privacy, is the principle that a person should have control over their personal data, including the ability to decide how public and private organisations collect, store, and use their data. It focuses on the rights of individuals to control or influence what data is collected about them, how it is used, by whom, and for what purposes. **Data security** refers to the practice of keeping data protected from corruption and unauthorised access, thereby ensuring privacy. It also refers to the range of measures and tools used for safeguarding data from unauthorised access, misuse, theft, and/or damage, such as encryption, authentication, access controls, network security measures (such as firewalls), and secure coding practices.

It is important to note that while data security is a crucial component of data privacy, the inverse is not necessarily true. A system can be highly secure yet still not respect privacy if it collects, uses, or shares data in ways that are inappropriate or that undermine respect for human rights.

Additional terms and definitions:

Data minimisation is the process of limiting the collection of personal information to what is directly relevant and necessarily to accomplish a specified purpose. This data should also only be retained for as long as is necessary to fulfil that purpose.

Data anonymisation is process of ensuring that data does not relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a manner that the data subject is not – or is no longer – identifiable.

Data encryption is the process of translating data into complex codes to hide privileged information, verify complete transmission, or verify the sender's identity. Encrypted data cannot be read without the decryption key or algorithm, which is usually stored separately and cannot be calculated based on other data elements in the same data set.

3 KEY PLAYERS

A wide range of organisations globally play a role in data oversight.

Global organisations like the United Nations General Assembly (UNGA), the UN System Chief Executives Board for Coordination (UN CEB), the Organisation for Economic Co-operation and Development (OECD), and the World Bank play a role in developing guidance and setting expectations on data oversight.

Non-governmental organisations such as the Data Management Association (DAMA International) and the World Economic Forum (WEF) also provide guidance, including developing standards, defining key concepts, and developing data strategies and frameworks.

National governments and agencies also engage in this work, including the European Union (such as through the creation of the GDPR), the National Institute of Standards and Technology (NIST), the US Securities and Exchange Commission (SEC), the Canadian Centre for Cyber Security, and more.

Private companies like IBM, PwC, Microsoft, and others have also developed and shared frameworks and tools to address industry-specific data-related challenges.

4 COMMITTING TO TAKE ACTION – MID- AND LONG-TERM COMMITMENTS

Committing to take action on **Data Oversight** can include addressing many of the key topics listed above. The mid- and long-term commitments that your organisation elects to make should be based on your identified priorities, areas of greatest impact, and your capacity to undertake the work required. It is important to note that this section does not provide *all* possible mid- and long-term goals related to this issue, but rather a sample of the goals that were most frequently adopted by companies in our research.

Common mid- and long-term goals and/or commitments on **Data Oversight** include variations of the following:

Long-term commitment: We will create and maintain a healthy digital ecosystem that ensures the responsible, ethical, and effective use of data.

- We will develop a governance body and framework to oversee data-related needs and activities.
- We will establish a strong and effective data oversight strategy that enables us to leverage data as a critical asset.
- We will build a strong data culture that enables employees at all levels to understand and use data in ways that improve efficiency and drive innovation.

Long-term commitment: We will maintain effective and ethical data oversight by ensuring data protection, including both data privacy and data security.

- We will uphold and advance the right to privacy within our operations, as defined by key authorities on human rights.
- We will adopt or adapt recognised data protection principles, such as for data collection and use limitations, data quality, purpose specification, security safeguards, openness, individual participation, and accountability.
- We will ensure that all data collected is protected from unauthorised access and will prevent the misuse of data and other malicious cyber activities.
- We will ensure compliance with the evolving set of global and regional data regulations.

Long-term commitment: Within our value chain, we will promote data protection and the need to uphold and advance the right to data privacy.

- We will ensure our value chain partners uphold and advance the right to privacy, as defined by key authorities on human rights.
- We will support our value chain partners to prevent and address cybersecurity risks.
- We will monitor our value chain for compliance with the evolving set of global and regional data regulations.

Are you setting new commitments or interested in benchmarking your commitments against leading practice? To help advance progress in credible corporate sustainability positions and commitments, the Embedding Project maintains a public position statement database containing leading sustainability commitments set by large companies globally. Explore our Position Database for more mid- and long-term commitments on data oversight.

5 HOW TO GET THERE – PROCESS-BASED INTERIM TARGETS

Note: The following proposed timelines are only for guidance and are based on the pace outlined by other companies. The timeframe for actions and work for each step needs to be embedded in your organisational context, which may require different time allocations.

These examples of mid- and long-term commitments are not intended to be strict and prescriptive, nor do they identify the full range of potential (and crucial) actions that an organisation must take to ensure effective data oversight. These examples should be viewed as a starting point to provoke constructive conversations and should be adapted and supplemented with actions that reflect both your organisation's maturity on data oversight and your unique operating context (as well as that of your value chain partners). Further, implementing these steps may require significant organisational learning; any commitments should reflect urgency.

*The sequence outlined below assumes that your company has significant potential impacts related to **data oversight** within its direct operations and that you will begin to engage with your value chain after learning and taking action to get your own house in order. Companies with greater potential impacts within their value chain may (and likely should) opt to engage with value chain partners at a much earlier stage. Your company may need to start at a qualitative level with impacts and dependencies on data oversight to understand where data oversight is crucially interlinked within your operations and value chain, use this understanding to prioritise areas for action, and then begin to undertake the process below to address the most material issues.*

YEAR 1: ESTABLISH A DATA GOVERNANCE BODY AND FRAMEWORK

Data oversight involves a comprehensive range of actions and decisions, and it is important to establish and empower effective leadership to guide your data strategy.

Begin by empowering a data governance body (commonly referred to as Data Governance Boards, Data Strategy Teams, or Data Councils) with authority and oversight over the management of your organisation's data assets. This governance body is generally led by the Chief Data Officer (CDO). Consider creating a data governance charter to formalise and assign key roles, responsibilities, and expectations for developing, overseeing, and coordinating data stewardship and data protection.

Your governance body should then create, adopt, and adapt (as necessary) a governance framework. This will include identifying the scope of data assets that need to be identified and managed and setting and enforcing priorities for managing and using data as a strategic asset. Your governance body should establish policies, procedures, and rules for the creation, acquisition, privacy, integrity, security, quality, and use of data and information. Other key tasks will include establishing a process for monitoring compliance with policies, standards, and responsibilities throughout the information lifecycle; identifying appropriate standards and reporting structures to ensure that data assets are properly and transparently managed; establishing intervals for regular updates about the data governance body's impact; and holding members accountable for elevating the organisation's data oversight maturity.

CASE STUDY: Apple provides comprehensive information on how privacy governance is structured within their organisation, including roles, hierarchies, and responsibilities for a range of data and privacy-specific oversight activities. They also explain the training that employees are required to take to ensure that the company can meet its commitment to respect human rights and conduct business ethically, honestly, and in compliance with applicable laws and regulations, such as the GDPR and CCPA.

YEAR 1: ENSURE DATA PROTECTION IN THE CONTEXTS WHERE YOU OPERATE

You will want to clarify the legal scope of the right to privacy in the regions where you operate. Ideally, much of this work will have already been explored and/or completed as a part of your organisation's regular compliance processes. It is also important that individuals understand their data-related rights. In addition to taking appropriate measures to protect every individual's right to privacy, consider transparently explaining to users what information you collect; why and how it is collected, stored, used, and protected; and how users can access, update, manage, export, and delete their information.

Ideally, your cybersecurity strategy will be embedded into your overall business strategy so that it supports and enhances your ability to achieve your business goals. Key data protection commitments to consider include protecting the confidentiality, integrity, and availability of sensitive data; safeguarding business continuity, including the ability to respond to incidences and recover from disasters; and ensuring regulatory compliance, all while considering and managing potential risks and costs.

Tangible steps include implementing administrative, technical, and physical safeguards to help protect the confidentiality, integrity, and availability of systems, networks, and information. If you have not already done so, consider implementing industry-recognised security practices such as robust password protections, multi-factor authentication, and passkeys; appropriately configured firewalls; network monitoring and intrusion detection systems; and technical and administrative access controls to limit who has access to personal information. You can improve privacy protections by limiting the personal information that is used and employ data aggregation, anonymisation, and encryption techniques (both in transit and at rest) to protect private information.

CASE STUDY: In the wake of one of the largest data breaches in history, Capital One published a comprehensive release that explained what happened; the impact on customers, including details on the data that was obtained; the steps Capital One has taken to strengthen their cybersecurity; and more.

Examples of process-based targets for Year 1:

- By 20[XX], we will understand and comply with applicable laws and regulations (national, regional, and local) for data protection, including both data privacy and data security.
- By 20[XX], we will actively maintain a formal, modern information security policy based on the recognised industry security standards and aligned with relevant security frameworks, such as the NIST Cybersecurity Framework.
- By 20[XX], we will develop a formal cybersecurity awareness program to ensure all personnel (as well as designated contractors) are provided with appropriate data protection knowledge and are adequately trained to perform their duties and responsibilities in alignment with data protection policies.
- By 20[XX], we will establish information security teams to promote and assist in the enforcement of our data protection policies and practices.
- By 20[XX], we will develop and implement controls to oversee and restrict physical access to facilities housing data systems and infrastructure to authorised personnel.
- By 20[XX], we will establish an integrated vulnerability management program and perform rigorous and routine internal and external vulnerability scans.
- By 20[XX], we will develop and maintain an adaptive and actionable data incident response plan to ensure timely reaction to security events.
- By 20[XX], we will develop and maintain business continuity and disaster recovery protocols to enhance our ability to respond to significant events that might disrupt our systems, networks, and facilities, or may otherwise impair our ability to provide service.
- By 20[XX], we will establish a data literacy plan.

YEAR 2: DEVELOP A POSITION STATEMENT ON DATA PROTECTION

Writing position statements creates time and space for senior leaders and the board to have deep conversations about sustainability issues. They promote productive debate, provide direction to employees and management to act, clarify expectations, and support accountability. There are several data oversight topics that may warrant a position statement, such as data privacy and data security.

Given growing regulatory requirements and public expectations, you may want to prioritise a position statement on data privacy. Your statement should explain the issue of data privacy, including the importance of data oversight to society at large, key trends, and the actions and commitments that relevant communities, governments, and industries are taking to address this issue. Your statement should explain key thresholds by referencing key sources of authority that articulate and affirm privacy as a human right, and the collective action that is needed to uphold this right. Link the issues of data privacy and oversight to your business, including its strategic impact and the constraints it will place on your decision-making, as well as your direct operational and value chain impacts on these issues. Finally, clarify how you will do your part to address your direct and indirect impacts and how you will support positive systems change. You can also clarify future accountability by disclosing key information about your data governance body and framework.

To dive deeper into developing credible position statements, read our guide.

CASE STUDY: Johnson & Johnson has written a position on data privacy that explains the importance of data privacy, both to their business strategy and to society at large. They also articulate their guiding principles and their commitment to fair and transparent data processing practices.

YEAR 2: CONDUCT A DATA MATURITY ASSESSMENT

As your data oversight efforts take root, you will want to review and benchmark against documented best practices. Your data governance body should create, adopt, or adapt a data maturity assessment model and engage with key stakeholders to solicit input on the current state of your data oversight activities.

Identify gaps and areas to prioritise for improvement. This includes analysing policies, procedures, and operations related to data oversight, including (but not limited to) data governance, data stewardship, data infrastructure, data culture, staff skills and capacity, and compliance with law and policy. This also includes assessing roles and their responsibilities to determine how relevant and appropriate they remain.

After conducting the assessment, your data governance body can evaluate the results and make recommendations for next steps. They can also evaluate the usefulness of the model and consider recommendations for improvements.

Examples of process-based targets for Year 2:

- By 20[XX], we will develop a clear commitment to respect the right to privacy.
- By 20[XX], we will assess the current state of the organisation's data oversight. We will identify barriers and gaps to leveraging data, such as challenges related to data management, data integration, and workflows.
- By 20[XX], we will develop a clear understanding of the quality of our organisation's sustainability data and how it flows between different areas of our business and connect data and analytics to priority business outcomes.
- By 20[XX], we will scale our data culture and capacity by hiring and reskilling talent.
- By 20[XX], we will develop a plan for closing the skills gap by providing ongoing training to keep pace with advances in technology and service expectations, as well as adjusting education and experience requirements to fill roles.
- By 20[XX], we will establish a regular process for reviewing and updating our data governance framework and membership.
- By 20[XX], we will benchmark our current data oversight policies, practices, narrative, and culture against industry peers, leaders in data oversight, and against expectations and obligations related to the right to privacy.
- By 20[XX], we will perform a data audit, including understanding what data our company collects, from whom, and under what circumstances, as well as how it is stored, used, shared, and protected.

YEAR 3: EXTEND YOUR LEARNINGS TO YOUR VALUE CHAIN

It is important to account for cyber risks within your value chain, including when contracting with customers and service providers. It is also important to share the knowledge and skills your organisation has developed to promote a broad and consistent understanding of data oversight, and especially of data protection.

Consider how your procurement practices and relationships with suppliers can help strengthen their capacity to implement strong data governance and cybersecurity measures and prevent risks related to violating the right to privacy.

This may include support for the development of their data strategy by sharing the learnings from your own journey, capacity building opportunities, or co-funding initiatives that foster respect for the right to privacy. Build contractual agreements in ways that enable and encourage suppliers to respect the right to privacy, and include expectations to respect privacy in your supplier selection criteria. Also consider requirements for suppliers to implement modern and comprehensive cybersecurity measures to ensure that the risk of cyber-attacks through third parties is kept to a minimum. Provide detailed criteria for how suppliers must respect the right to privacy, including – at a minimum – the laws and regulations that your company complies with.

CASE STUDY: Rockwell Automation launched a new cybersecurity initiative after multiple small- and medium-sized suppliers informed them of product delivery delays due to ransomware attacks. In partnership with Dragos, an industrial cybersecurity company with comprehensive experience in cybersecurity solutions for operational technology (OT), Rockwell's multi-year initiative educated suppliers on cybersecurity and made cybersecurity contractually required. The result was a significant improvement in Rockwell's end-to-end supply chain resiliency, customer protection, delivery times, company revenue, and reputation.

YEAR 3: UNDERSTAND ROOT CAUSES AND PRIORITISE AREAS FOR ACTION IN YOUR VALUE CHAIN

For many companies, potential data privacy and cybersecurity impacts will reside within their value chain. Data privacy and cybersecurity have become critical concerns in today's digital value chain landscape. Although value chain digitalisation can enhance transparency and improve operational efficiency, it also increases the risk of data breaches and cyberattacks.

Explore areas of vulnerability within your value chain to better understand the actions that must be prioritised. It is also important to determine the applicability of global data privacy and protection laws and regulations to companies within your value chain. Failure of value chain members to comply may expose your organisation to fines and security risks, as well as risks to reputation in the event of a security incident.

Begin by clearly defining data handling guidelines for third-party vendors and other value chain partners. Ensure they are only collecting and sharing necessary data for specific purposes and establish strong contracts that hold them accountable for data protection. Conduct regular audits of value chain partners and leverage cybersecurity tools and practices to protect data in transit and during storage.

Examples of process-based targets for Year 3:

- By 20[XX], we will develop an action plan to ensure the right to privacy is understood within our value chain.
- By 20[XX], we will build contractual agreements in ways that enable and, where possible, require all suppliers to respect the right to privacy.
- By 20[XX], we will create a Supplier Data Code of Conduct that outlines data privacy and data security requirements for all suppliers.
- By 20[XX], we will use contractual and other measures to obtain suppliers' compliance with appropriate information security requirements.

RESOURCES

GUIDANCE

Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda sets out general guidance on data privacy, data protection and data ethics for the United Nations Development Group (UNDG) concerning the use of big data, collected in real time by private sector entities as part of their business offerings, and shared with UNDG members for the purposes of strengthening operational implementation of their programmes to support the achievement of the 2030 Agenda.

The UN System Chief Executives Board for Coordination's (CEB) Principles on Personal Data Protection and Privacy set out a basic framework for the processing of personal data by, or on behalf of, the United Nations System Organisations in carrying out their mandated activities. There is also a Supplemental easy-access summary of the principles.

The Global Cybersecurity Outlook 2026 examines the cybersecurity trends that will affect economies and societies in the year to come, including advancements in AI and emerging technologies, geopolitical tensions, cybercrime sophistication, the cyber skills gap, regulatory requirements, and supply chain interdependencies. The report is divided into two main section: CEO priorities in a shifting cyber landscape, and trends reshaping cybersecurity. This report will be especially beneficial for sustainability, risk, security, and technology professionals that want to summarise prominent near-future IT- and data-related threats for senior leaders.

TOOLS

NIST Privacy Framework is a voluntary tool that can help you to identify and manage privacy risk and to bring privacy risk into parity with your broader enterprise risk portfolio. The framework is composed of three components: Core, Organisational Profiles, and Tiers. The "Framework Core" provides an increasingly granular set of activities and outcomes that enable organisational dialogue about managing privacy risk; "Organisational Profiles" are a selection of specific functions, categories, and subcategories from the Core that your organisation has prioritised to help manage privacy risk; and "Tiers" support communication about whether your organisation has sufficient processes and resources in place to manage privacy risk.

NIST Cybersecurity Framework can help you better manage cybersecurity risks. It provides a common language and systematic methodology for managing this risk and features a three-component framework. The "Framework Core" unpacks five pillars of a holistic cybersecurity program (Identify, Protect, Detect, Respond, and Recover); the "Implementation Tiers" help you to prioritise your cybersecurity program activities, as per your goals, risk appetite, and budget; and the "Profiles" section helps you to identify areas to improve.

NIST AI Risk Management Framework is a non-sector-specific, use-case agnostic, and practical framework to help individuals, organisations, and societies manage risks related to artificial intelligence. Intended for voluntary use, the AI Risk Management Framework

(RMF) was created to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. This framework is centred around four core functions that organise AI risk management activities at their highest level, enabling you to better govern, map, measure, and manage these risks.

STANDARDS

OECD Privacy Guidelines are the first internationally agreed-upon set of data protection principles, and they have inspired similar frameworks around the globe. They set out eight Basic Principles of National Application, including collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

Legal framework of EU data protection explains how EU data protection legislation is comprised of the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), and the Data Protection Regulation for EU institutions, bodies, offices, and agencies (EUDPR).

General Data Protection Regulation (GDPR) is an EU law that governs how organisations, both within and outside of the EU, handle the personal data of EU residents, ensuring data protection and control for individuals. Built on established and widely accepted privacy principles, such as purpose limitation, lawfulness, transparency, integrity, and confidentiality, the GDPR strengthens existing privacy and security requirements, including requirements for notice and consent, technical and operational security measures, and cross-border data flow mechanisms. The GDPR also formalises new privacy principles, such as accountability and data minimisation.

For Indigenous data sovereignty, the First Nations Principles of OCAP (ownership, control, access, possession) assert that Indigenous Peoples have control over data collection processes, and that they own and control how this information can be used.

For sharing, using, and reusing data, the FAIR Guiding Principles for scientific data management and stewardship provide guidelines to improve the Findability, Accessibility, Interoperability, and Reuse of digital assets. As a result of the increase in volume, complexity, and creation speed of data, the principles emphasise the capacity of computational systems to find, access, interoperate, and reuse data with limited (or without) human intervention.

Global Indigenous Digital Alliance (GIDA) has developed the CARE principles (collective benefit, authority to control, responsibility, ethics) to prioritise Indigenous rights, interests, and control over their data and knowledge, and to ensure that Indigenous data is used in ways that align with Indigenous values and aspirations.

Explore more curated resources on Data Oversight on our website.

ACKNOWLEDGEMENTS

This research was supported by
Social Sciences and Humanities Research Council of Canada (SSHRC)

Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada
Canada

And by contributions from our corporate partners
https://embeddingproject.org/our-community/

The Embedding Project is hosted by
Beedie School of Business at Simon Fraser University

SFU BEEDIE SCHOOL OF BUSINESS