COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2024
A Data Privacy Compliance Program Primer: A Snapshot of Data Privacy Regulations, Risks, and Compliance and Risk Management Effectiveness Strategies

By Deborah Lynne Adleman and Jennifer Ruehr[1]

As privacy and data protection[2] risks continue to be among the top risks for many organizations, compliance and risk leaders are increasingly expected to understand what these risks are and how their organization is preventing, detecting, and responding to (mitigating) this specialized risk landscape. This chapter provides a snapshot of the privacy and data protection landscape, a road map for building or assessing the privacy and risk management compliance program, and a checklist for the program's effectiveness (collectively referred to as privacy compliance program).

Personal Data Defined

Privacy compliance programs are focused on how personal data is collected, used, processed, shared, stored, and disposed of consistent with applicable laws, regulations, professional practice requirements, individuals' expectations, and contractual obligations. The first step for the privacy compliance program is understanding the nature of personal data the organization is processing.

From Europe to Latin America, Canada, and the United States to Asia-Pacific, there are differences in personal data definitions, as local, state, federal, and international laws and regulations attempt to address the expanding e-commerce ecosystem and the ability to target or identify individuals using indirectly identifiable information, such as unique identifiers like device IDs, internet protocol addresses, or location data (which, if misused, can create risk to the individual's information). Below are some examples of the different definitions of personal data.[3]

Law[4]	Personal Data Definition
General Data Protection Regulation (GDPR)	"Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[5] pertaining to individuals in Europe.[6]

Law[4]	Personal Data Definition
Personal Information Protection and Electronic Documents Act (PIPEDA)	"Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: • Age, name, ID numbers, income, ethnic origin, or blood type; • Opinions, evaluations, comments, social status, or disciplinary actions; and • Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs)."[7]
Brazil's Law No. 13,709/18, or the Personal Data Protection Law (LGPD)	"Personal data: information regarding an identified or identifiable natural person.'[8]
California Consumer Privacy Act (CCPA)	"Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, [information that could be] reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."[9]
Virginia Consumer Data Protection Act	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include de-identified data or publicly available information.[10]
Health Insurance Portability and Accountability Act (HIPAA)	Individually identifiable health information is information, including demographic data, that relates to the individual's "past, present, or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."[11]

In addition to these definitions, many laws and regulations have a specific definition for "special" or "sensitive" information that requires additional controls when processed by an organization. Given the variation in these definitions, compliance and risk professionals should begin by understanding which of these personal data types flow through their particular business environment and whether the personal data is "sensitive" data under the applicable law or regulation.

General Data Privacy Principles and Risks

Privacy Principles

To demonstrate an effective privacy compliance program, compliance and risk professionals should start by analyzing and documenting the types of personal data that the organization is processing, including the data flows (i.e., technologies, systems, and processes). The Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[12] historically provided such a backbone. Next, it is important to understand the basic principles for how such data should be used and protected. Across this varied landscape, a common "minimum floor" of privacy principles and resulting expectations has emerged:

- Maintain the accuracy of the data.
- Process data consistent with only the original purpose of its collection and based on a lawful purpose reflecting the rights of individual data subjects.
- Process only the minimum data that is consistent with that processing.
- Limit access to, and disclosure of, the data to those persons or systems that demonstrate a business purpose for that processing.
- Maintain the security of the data for the duration of the processing.
- Include appropriate contractual clauses with entities processing the data.
- Document cross-border data transfers.
- Include systems, techniques, or processes (controls) designed to reduce privacy risks. This principle is known as "privacy by design and default," with such examples as encryption, anonymization, or other measures—all of which are designed to prevent harm.[13]
- Implement appropriate retention and deletion policies once the purpose of the processing has been achieved.

Privacy Risks

Once the compliance professional understands what personal data they are processing, the assets (systems/procedures) processing the data, where the data is being processed, and the core principles for that processing, the next step is understanding the inherent risks to the personal data that can occur as a result of that processing.

Privacy risk is frequently considered one of if not the highest enterprise organizational risk. Compliance and risk professionals will want to engage with senior leadership to confirm and assess how privacy is incorporated into the enterprise risk management process. This process will also include consideration for the organization's privacy risk appetite and tolerance.[14]

Foundational Privacy Risks

Although the likelihood and/or impact of risks will differ based on geography and sector, the majority of privacy risks connects to potential data breaches of some type, including inappropriate use, access, loss, disposal, or

disclosure of personal data. Some of those risks include:

- Violation of legal, regulatory, professional practice, and/or contractual obligations;
- Failure to adequately perform diligence on third parties and/or acquired entities that become the subject of a data breach;
- Removal of the ability to do business in an industry[15] or with a regulated group;
- Reduction of trust by stakeholders (i.e., employees, contractors, customers);
- Significant fines, penalties, or damages (monetary and non-monetary, including deletion of unlawfully collected personal data and technology derived from it[16]); and
- Liabilities arising from the failure to promptly notify potentially large groups of people in the event of a data breach (with its inherent complexities).

Privacy Risk and Reward: New and Emerging Technologies

Technology that uses personal data is central for most, if not many, business operations and business growth. Since most organizations will use personal data–infused technology, the compliance and risk professional will want to understand what the organization's risk appetite is (i.e., the amount and type of risk that the organization is willing to take through that technology processing of personal data in support of its key objectives, mission, and values). By aligning risk appetite with specific tolerance levels, putting proper controls in place to calibrate those risk appetites, testing those controls, and using technology itself to monitor the effectiveness of those controls, organizations can not only reduce their risk but potentially continue to enhance their operations and achieve their objectives. The risk and compliance leader is uniquely positioned to shepherd these processes.

As organizations develop, implement and/or purchase new technologies, their privacy risks may change. Embracing new technologies that process personal data requires new questions (e.g., What is the data integrity of those technologies? How has the organization examined the legacy data of the old technology that was replaced? What are the impacts of new data flows from the new technologies?)

Companies are eager to push forward and embrace new technologies that will enhance their operations, particularly in a post-COVID-19 environment. However, in their zeal, they may choose to push technology, including technology that processes personal data, forward without completing proper assessments.

Compliance and risk professionals should examine how the system development life cycle, procurement, and third-party risk management processes contemplate privacy risk. From third-party risk management to IT impact assessment or artificial intelligence ethics impact assessment, the compliance and risk leaders can underscore and play a key role in reminding the organization of the importance of diligence. New and emerging technologies also create the need for examination of and modifications to foundational compliance program components, such as policy, learning, awareness, and—broadly—change management.

Additionally, technologies are being developed with the specific intent to reduce privacy risk. The International Association of Privacy Professionals' *Privacy Tech Vendor Report*[17] provides compliance and risk professionals with an expansive list of vendors that not only mitigate privacy risk, but also enhance the performance of the privacy program. The Federal Trade Commission (FTC) enforcement actions span privacy and information security control requirements, demonstrating the increasing importance of addressing both of these in the above privacy risk identification and assessment process. The enforcement covers areas such as:

- Security, confidentiality, availability, and integrity of consumer's (including children's) personal data, including strength of the information security program;
- Accuracy of consumer privacy notices to avoid improper data sharing practices;
- Privacy shield principles for those companies who continue to assert participation in and, therefore, adherence to the principles;
- Artificial intelligence–related issues, specifically facial recognition limitations; and
- Information security controls, in particular for vendors (suppliers) processing personal data.

Cloud Computing

The breadth and scope with which organizations embrace cloud computing continues to evolve and expand, and with it, potential for privacy risk. As organizations create more data, their storage demands increase proportionately, resulting in the use of external solutions such as third-party cloud computing. Similarly, organizations requiring increases in processing power and/or data sources necessary to manage intelligent automation often result in the involvement of third-party suppliers. These types of technical factors can independently or in combination elevate the risk of improperly obtaining, storing, processing, and/or securing personal data. whether managed internally or by a third party.

The American Institute of Certified Public Accountants privacy management framework similarly discusses privacy risks with third-party cloud computing:

> "Outsourcing the management and operational support for systems and data processing to others…such as in cloud computing…increases the complexity of an organization's ability to address its information privacy requirements. Organizations are increasingly looking to move computing and data storage to other organizations and to outsource business processes and with it the activities related to information privacy. Organizations cannot delegate their responsibilities for protecting the privacy (of) information…related to its business processes."[18]

Artificial Intelligence: Generative AI, Machine Learning, and Privacy

As organizations embrace machine learning and the related disciplines as means to enhance business operations, they are required to consume large quantities of data to train their algorithms. As a result, organizations have to assess whether the controls they have in place to collect and process these large data sources—frequently including personal data—are strong enough to withstand the pressures imposed by the desire for the revenue and performance improvements. Furthermore, organizations have to assess how their controls are applied to third parties, including their vendors that similarly leverage AI, and have relied on customer data and unknown sources of data for training their algorithmic models.

Large Language Models (LLM) and the Generative AI (GAI) applications not only require large data sets to train their models and create their algorithms, they can expose the user to risks such as inadvertently sharing their own data to the GAI application. And, this data may in turn become training data which can be exploited by bad actors through known vulnerabilties such as prompt injection attacks (which is looking for training data by inputting prompts for which the algorithm hasn't been trained to reject) and other adversarial machine learning

techniques.[19] Also, organizations' staff may use outputs generated by these algorithms without validating them. Moreover, LLM and GAI may have collected data unlawfully, or at least without transparency, again exposing the user and the organization to potential risk. Lastly, as GAI is increasingly embedded into everyday tools such as simple presentation and document creation, organizations risk their staff again inadvertently either sharing proprietary information or personal data with these tools or not validating the output generated from these tools and making decisions that could have a legal impact on others.

Privacy-enhancing Technologies

Privacy-enhancing technologies (PETs) are examples of reducing privacy risk, which can include bringing the processing engine to the data (and removing the risk of centralization), bypassing the inherent limitations of anonymization by adding additional data to reduce re-identification risk, or allowing processing while the data is protected by encryption. In 2021, the United States House of Representatives introduced Bill S.224, Promoting Digital Privacy Technologies Act, which specifically encouraged development of PETs.[20] The European Union Agency for Cybersecurity, which works closely with the European Data Protection Board, continued the dialogue on PETs in January 2021, exploring their use across multiple industries, including financial and healthcare.[21] While these PETs are emerging, compliance officers should continue to watch how they can be consumed across their enterprise.[22]