Data Governance and Privacy by Design:
Guidelines for a Mature and Compliant Organizational Framework

By: Alan. L. Friel and Kyle R. Fath, Squire Patton Boggs
May 2021

For more information contact Alan.Friel@SquirePB.com

Data is many companies' most valuable digital asset. However, an increasing number of laws and regulations seek to regulate companies' collection, use and disclosure of data, particularly information that relates to or identifies an individual. If an organization responds to these laws by leaving it to a legal or compliance department to address, or by viewing compliance with them as a purely legal issue, then its ability to ensure compliance with such laws over the long term will be materially compromised. Moreover, it will miss an excellent opportunity to reduce business risk, reduce costs and increase the value of its data to the organization or exploit it in meaningful ways. It is therefore vital that organizations intimately understand the data they are collecting, processing, retaining, and sharing with third parties in order to protect the organization's brand and reputation, extract value from the data it maintains and comply with the ever-growing alphabet soup of laws to which they are subject.

Companies with clear visibility into their data inventory and documented, consistent practices will readily be able to apply data governance standards to their data practices and make sound business decisions that meet or exceed those standards.

What is less apparent, however, to many lawyers, business leaders, and even information professionals, is exactly how to manage information and its privacy and security properly. Many data governance and privacy standards, such as Privacy by Design (PbD) (discussed in further detail below), were best practices a mere five or six years ago. Since then, data privacy laws such as the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), and Virginia's Consumer Data Protection Act (CDPA) have effectively codified many data governance practices and provided concrete standards on which companies should – and in some cases are legally required to – base a mature data governance program. This article suggests an approach for how to design and run a data governance and Privacy by Design program that is right for your company.

PROGRAM ELEMENTS AND FRAMEWORK

An effective privacy, data protection, and information governance program (which we will refer to collectively as a "data governance program") requires a multi-disciplinary approach with a mandate from the Board and C-suite, and ongoing assessment and updating as standards and legal requirements change. What is legally required, cost beneficial, and otherwise reasonable under the circumstances will differ based on company size, industry, jurisdictional footprint, and corporate philosophy. Accordingly, data governance programs must be developed and evaluated individually - sadly, there is no boilerplate, one-size-fits-all model. However, there are paradigms, elements and best practices, discussed below, that all good programs have in common.

Privacy and data security are often referred to as opposite sides of the same data governance coin. While this metaphor does help visualize the similarities and differences between privacy and data security and their inextricable links to each other, it ignores other aspects of data governance all together. When looked at instead as three indispensable legs of the data governance stool, the role of each is better understood:

1. **Privacy**. This relates to an individual's (consumers and employees typically) ability, and in some jurisdictions, right to control the collection, use, and disclosure of their "personal information" or "personally identifiable information" - terms defined in a number of ways depending upon context and jurisdiction.

2. **Information Management**. This relates to the management not just of personal information, but of all data, including data that is purely business information but may be of even greater sensitivity than personal information (*e.g.*, trade secrets, evidence in a pending litigation, etc.).

3. **Data Security**. This relates to protecting the data itself from unauthorized access, use, loss, corruption or destruction; providing policies, practices, systems, technical and operational controls, and safeguards to enforce access restrictions; and evaluating and monitoring this security and responding to suspected or actual security compromises. A violation of privacy, or of information governance policy, may or may not necessarily be a data security incident.

These three components of data governance need to be considered together in a collaborative manner, even where, as is typical in large organizations, each has its own domain. This can be accomplished through bringing together all data stakeholders across domains and developing collaboratively shared policies, goals and tools. Only in this way can an integrated and overall data governance program be developed and implemented.

Breaking data governance framework principles down to the most general topics, a data governance program can be organized, evaluated and operated, and risk assessed and mitigated, based on just five categories: 1) Governance; 2) Transparency and Choice; 3) Security and Control; 4) Third Party Risk; and 5) Accountability:

- **Governance**. The company understands the data it has, its legal, self-regulatory, and third-party obligations regarding the data, and the business choices it has regarding it. Based on this knowledge, it develops a data management strategy conveyed in a program mission statement, which guides the development and implementation of program policies, procedures, and notices. Program management is vested with appropriate authority and resources to ensure the ability to ensure accountability and ongoing assessment and improvement, with coverage over all parties with access to company data, including vendors and other third parties.

- **Transparency and Choice**. The company's policies and practices are apparent to data subjects and data stakeholders. Data subjects should have reasonable and accurate notice regarding the collection, use, dissemination, maintenance and security of data about them, with specificity of purpose, particularly in regard to their personal information and any choices available to them regarding such information.

Depending on the jurisdiction, organizations must provide data subjects choices as to the processing of their personal data and may even be required to obtain consent for certain types of processing. To the extent data subjects are required to be given a choice, or it is otherwise offered, the company gives meaningful notice of the choices, a reasonable method for exercising them, and in fact honors those choices.

- **Security and Control**. Data security is about data control, and since the 1960's the model of data security has been the C-I-A triad: *Confidentiality* (prevent unauthorized access); *Integrity* (prevent unauthorized and unintentional alteration or deletion); and *Availability* (data remains available to authorized users). A company should appropriately limit the access and use of its data and take reasonable measures, which will depend on the sensitivity of the data, to protect against unauthorized access and use, and from corruption, loss or unintended destruction. Minimizing data collected and retained, and its use, reduces risk. Training and awareness, as well as technical and procedural steps to protect the data, are essential. The company should have an incident management and response plan, train on how to respond to an incident, and evaluate what led to incidents when they occur and how to better prevent future incidents.

- **Third Party Risk.** The company has a comprehensive inventory and understanding of vendors and other third parties that are processing data on its behalf. This has become essential as new laws provide detailed requirements on the contract requirements for processing limitations and data protection on vendors (e.g., processors, contractors, and service providers), treat conforming transfers as "sales" or illegitimate transfers, and create safe harbors for compliant disclosures.

  As to each third party, the company maintains and, at defined intervals, updates an inventory of what data and for what purposes the third party is processing (among other things, depending on legal requirements). The appropriate stakeholders (e.g., privacy, security) are engaged early and systematically in the vendor intake process by procurement or the other department/stakeholder responsible for the vendor or other third party relationship.

  In addition, the company's stakeholders keep one another apprised of third party compliance requirements. Third parties such as "Big Tech" and other vendors, upon which many companies rely for advertising and other services, impose requirements on their customers arising out of their own compliance obligations. These obligations may be purely contractual, legal, or self-regulatory in nature. As part of communicating regularly and systematizing compliance with legal obligations, the company's applicable stakeholders address these third-party requirements. Legal and privacy stakeholders educate the business of the regulatory requirements and make recommendations. The business teams consider third party vendors' requirements and limitations in not only implementing processes and procedures that align with legal's recommendations, but also in educating privacy and legal, to further inform the privacy and legal advice given to the business.

Likewise, the legal and privacy function considers and understands third party requirements and limitations when recommending internal compliance processes and procedures. For example, Google is phasing out third-party cookies and Apple recently began requiring opt-in for “tracking” individuals. While privacy and legal are well aware of these actions being taken by Big Tech, as are business stakeholders, the business needs to keep privacy and legal apprised of the alternatives in order for privacy and legal to assess and advise on the legal implications of the same. Many other examples abound of these “product counseling” issues.

- **Accountability**. The company communicates its policies and procedures to those it allows to access or maintain its data (including employees, vendors and other third parties), monitors for compliance, and enforces its standards and requirements. The company has known and accessible procedures to address complaints and disputes.

  The specific program policies and practices that will be fleshed out within each of the above categories will depend upon the laws and self-regulatory schemes that may be applicable to a company, as well as business judgment decisions as to how protective or exploitive a company desires to be of its data, within the limitations of applicable law.

OPERATIONAL BENEFITS OF GOOD DATA GOVERNANCE

Beyond legal compliance and brand protection, a systematic data governance program provides several benefits to the business. Some of these benefits include:

- Improved confidence in the quality of the organization’s data- information that is out-of-date, redundant or incomplete can result in faulty strategy and damage to customer relations;
- Better, more comprehensive analysis from consistent, uniform data across the organization;
- Clear rules for change management that help the business and IT become more agile and scalable;
- Reduced data management costs through the implementation of centralized controls and processes; and
- Increased efficiency through the ability to reuse processes and data.

STAKEHOLDERS AND THEIR ROLE

There are typically many data stakeholders, each with different relationships with a company’s data, and as such potentially different viewpoints toward how it should be collected, used, shared, protected and maintained. Only through involvement of all these stakeholders will a company be able to implement and maintain a comprehensive data governance program that meets company-wide needs and obligations. We recommend that a program’s mandate and governance structure be established with input from each of these stakeholders. This will make it more likely that complete information is gathered, and all stakeholders’ interests are considered. It also makes governance more effective and efficient.

While all these stakeholders need to be intimately involved in program development and operations, frequently through a committee structure, programs work best with ultimate responsibility invested in a single senior-level executive with documented responsibility for overseeing the program and reporting directly to the Board, CEO or executive management team. In some organizations, the executive's annual performance-based compensation is based in part on the executive meeting certain clearly established goals with respect to the data governance program.

With the increasing need to address privacy compliance, it is now very common for organizations to employ at least one privacy professional, whether it is a privacy counsel or non-lawyer data privacy professional. Often the privacy counsel or professional either also has the title, or effectively serves in the role, of Chief Privacy Officer (CPO). The Chief Information Officer/Chief Information Security Officer (CIO/CISO) is often the closest to an organization's data, with an intimate understanding of its internal systems and third party relationships, and is therefore a key person on any such committee.

Sometimes, particularly in larger organizations, there is a leadership team comprised of the CIO/CISO, a CPO, and potentially one or more other executives, such as the head of Regulatory Compliance and/or Risk Management. This team may share overall management responsibility or represent a second level of subject matter management reporting up to a single program leader. Multi-nationals and conglomerates may need various levels of structure, at for instance, divisional/subsidiary levels and/or jurisdictional levels. For such organizations, we recommend including representatives of parent company management to improve oversight and accountability and help avoid discrepancies in policy or practice not justified by business or legal considerations. Each company's size, footprint, management structure, and internal politics will drive what will be the most likely effective governance structure. However, for effective governance and accountability, a program needs both top down and bottom up involvement and the participation of the following stakeholders:

- **IT**. Information technology procures and maintains the company's information systems and vendors. Coordination is essential to ensure an effective and efficient data governance program. For technology-driven companies, IT may also be involved with, or responsible for, development of products that include personal information. As such, it has an essential role in facilitating the gathering of facts for privacy impact assessments and data security assessments and implementing Privacy by Design - important data protection program practices described below.

- **IS**. Information security is responsible for preventing unauthorized access to information systems and for helping ensure that sensitive data is restricted to access-controlled systems. This includes employing privacy and security enhancing technologies and data leakage prevention tools (where permitted by local law; some jurisdictions limit employee monitoring) and educating employees on data protection policies and best practices. IS monitors ongoing access control and accordingly is typically the first to become aware of potential and actual breaches and incidents and is crucial to facilitating prompt and appropriate response.

- **Privacy**. After being on the backburner for most organizations other than those subject to specific sectoral laws (e.g., HIPAA), consumer privacy is now at the forefront of most companies' compliance concerns, in large part because of the GDPR and the CCPA. Following California's lead, an ever-growing number of U.S. states have enacted or are considering enacting data protection laws that impose obligations on companies regarding personal information. These obligations may include notice, choice, consent, usage limitations, transfer limitations, retention limitations, rights of individuals to access, review, change and/or delete their data and the obligation to reasonably secure the data and give notice of unauthorized access or use.

Privacy by Design (PbD) has gone from a best practice employed by a select number of organizations to a *de facto* legal requirement with which most companies will have to comply, beginning in 2023.

Both CPRA and CDPA have strict purpose, proportionality, and minimization obligations, and CPRA requires the disclosure of retention periods (or, if not then "possible," how that period will be determined), by category of data, at the point of collection. As a result, covered businesses will need to develop very detailed retention schedules that include purposes of processing and that are tied to categories of data, as well as a defensible destruction program. This goes well beyond what public companies must have in the way of retention programs and schedules under the Sarbanes-Oxley Act and SEC regulations, though these are a good starting point. Further, since the CPRA requires such retention schedules be available for consumers to review at the points of data collection, it will be readily apparent to the AG and CalPPA, by merely sweeping website privacy notices, which companies have insufficient retention schedules.

The CPRA requires the collection, use, retention, and sharing of personal information to be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed…." While data minimization is generally considered best practice in the United States, this concept had not been broadly codified prior to the CPRA. Virginia's CDPA also codifies data minimization, and provides that controllers must limit the collection of personal data to that which is "adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed." The CPRA also reinforces that personal information cannot be used in a manner that is "incompatible with the disclosed purpose for which the personal information was collected" without providing the consumer with notice.

While PbD as a best practice certainly enables companies to address the above-mentioned obligations, the CPRA and Virginia's CDPA have effectively codified it into law. These requirements, among others, will require companies to not only attain facial compliance through privacy notices and elsewhere but also to apply their publicly stated retention periods and processing purposes to internal data practices and vendor/third party management across their organizations. Without applying PbD to all personal information collected across an organization, it will not be possible for companies to comply with these and future privacy regulations.

These requirements justify companies having a go-to privacy expert that is among the leaders of the data governance program, and developing an appreciation for privacy considerations at all levels and within all departments of the organization. In addition, for many types of organizations, a privacy and data governance committee may be in order.

- **Legal**. While a non-lawyer privacy professional certainly can be equipped for many privacy-related duties, an in-house or outside counsel expert in privacy and data protection law is necessary to advise on what legal, self-regulatory, and contractual obligations relate to company data, and draft company data practice policies and notices and contractual obligations for company vendors that have access to its data. Such counsel should also be involved in reviewing the design and functionality of products or services that involve the use of personal information. The expertise of privacy and data protection lawyers should also be called upon to advise on the legal implications of facts arising out of privacy impact and data security assessments and privacy and/or security breaches and other incidents. The expertise of lawyers is also helpful in designing appropriate record retention and destruction policies and advising on how data policies and practices may impact the rights of consumers and employees. Using outside counsel to manage assessments may protect some of the resulting work product with the benefit of the attorney-client privilege.

- **Procurement**. Procurement can communicate to vendors their privacy and data protection obligations and work with legal to ensure contractual commitments and indemnification. The group can also assist in evaluating the capability of vendors and suppliers to meet the company's privacy and data protection obligations.

- **Records**. All companies have some process for maintaining business records. The management of this function, which is typically carried out by the IT department, should include records retention and destruction management. Mature records programs are information governance programs and, where well integrated with privacy and security, can potentially serve as the umbrella for all data management program aspects. However, in most companies, records are a relatively low-level administrative function, the leadership of which lacks the clout to effectively manage an overall data management program and all of its stakeholders. Nonetheless, records are an essential stakeholder and resource.

- **Internal Audit**. Public companies may have an independent or semi-independent audit group reporting to the Board, the Board having ultimate responsibility for data governance. If so, internal auditors can be helpful with assessments, audits and program evaluations.

- **Regulatory Compliance/Ethics**. Regulatory compliance and ethics groups help establish and enforce the external and internal legal and regulatory obligations applicable to the company's activities, and those of its employees, suppliers and vendors. Given the overlap between public companies' retention obligations under the Sarbanes-Oxley Act, SEC regulations and the new mandates under state privacy laws, participation from the compliance department of these companies will be necessary as part of a data governance program. Moreover, given the heightened stakes for privacy and data protection compliance generally, privacy and data protection obligations should be part of his group's responsibilities.

- **HR**. Human resources is typically the repository of vast amounts of personal data of candidates and employees, and much of it sensitive. It also is the primary voice for most companies to communicate employee policy. With HR data in scope in the EU under the GDPR, and coming into scope in the U.S. under the CPRA at the beginning of 2023, the HR department is an important resource for privacy-related issues. However, many HR professionals and labor and employment lawyers, outside of Europe and countries with GDPR-molded regimes, are simply unaware of the impact of CCPA/CPRA on their data, as they do not think of their data subjects as "consumers." HR professionals also have a training role and can be crucial in helping educate employees on data protection policies and practices. HR can serve as an effective reporting structure for policy violations and for incidents, especially where an employee's complaint or report would implicate a supervisor. Finally, HR professionals should have knowledge of employee privacy rights under applicable laws.

- **Security**. Physical security is as important as information security in maintaining effective data protection. Involvement of security leadership, such as the CISO, is vital to an effective governance program.
- **Marketing**. Data governance is considered in any short-term plays or long-term marketing strategies. The marketing department systematically runs new projects and use cases by privacy and legal as a matter of course.

  Privacy regulation is aimed directly at the limiting the exploitation of data for marketing and advertising purposes. The GDPR requires consent for most marketing activities, broadly speaking, the CCPA allows consumers to opt out of the "sale" of personal information (including that which applies and occurs in the marketing and advertising contexts), and the CPRA and Virginia's CDPA will limit these activities even further. Consumer data is not the only information implicated. Even B-to-B companies use databases of customer contacts that contain personal information, and the "B-to-B exemption" under the CPRA sunsets on January 1, 2023, meaning that such information is subject to the full scope of the law after that date. Marketing departments must keep this in mind as they make day-to-day decisions and plan long-term strategies.
- **Product**. The product team, also referred to as the development, "dev", or product development team, is responsible for designing the front-end user experience and the back-end functionality of products and services. Therefore, this team is not only necessary for technical implementation of certain legal requirements (e.g., posting policies and notices, passing opt-out signals to vendors, etc.) but often has an intimate understanding of an organization's data flows and vendor and other third party relationships. The product team in an organization with a mature data governance program is a key stakeholder with a consistent seat at the table when key decisions are made and processes are implemented, in particular as it relates to Privacy by Design.
- **PR/Communications**. This group can assist with both internal educational messaging to promote program compliance and external communication in the event of an incident or breach.
- **Finance**. In order for an organization's data governance program to reach a mature state, the various groups enumerated above will need adequate budget to fulfill their responsibilities, and the company needs a contingency budget for responding to breaches and other incidents. In smaller companies, finance may also handle the roles of procurement and risk management.
- **Risk Management**. Companies with risk management functions may task them with evaluating risks and making cost-benefit recommendations, managing a business continuity plan, and/or making decisions as to what insurance, including cyber-liability insurance, the company will maintain and what it will require of its suppliers and vendors.

A program needs the participation of all of these stakeholders to be successful, and a governance structure to manage their participation and hold them accountable.

UNDERSTANDING COMPANY DATA AND DATA OBLIGATIONS AND PRACTICES

It is crucial that the company and its data stakeholders (especially those involved in program development and governance) understand the "who," "what," "where," "when" and "why" of its data. More particularly, an organization must understand what data it has, how it is collected, where it resides, its appropriate purposes and life cycle, what third parties have what interest in it, access to and involvement with it, how the company ensures appropriate protection and compliance with legal and other obligations, and that it is not inappropriately accessed, used or transferred. This is accomplished initially through inventories and assessments of data, data practices, and data obligations, and then application of appropriate controls on various data. This understanding is necessary to properly establish and document the company's overall strategic data governance mission, as well as to implement its vision through effective program management.

If not already undertaken, the process of data inventorying is a logical initial step for program development once the stakeholders are identified and organized. Thereafter, ongoing inventory updating is critical to keep a program effective. There are a number of tools that can be used to conduct and compile such inventories, including by automating the process, at least in part. However, use of data mapping programs (e.g., OneTrust, Truyo, Exterro, BigID, etc.) alone is insufficient, as the company still needs to know the purpose of that data, how it is used and by whom, and to establish rules around its retention, destruction, access, use and transfer. This can be done through surveys or interviews, which the software platforms can systematize and automate.

There are a number of vendors that provide consulting services that companies may utilize in addition to software vendors. Most sizeable organizations will need a combination of appropriate software vendor(s) and a number of staff (or outside consultants) dedicated to the data inventory process, working with the applicable stakeholders, in order to implement an initial data inventory project. Once the process is in place and the initial inventory done, most companies designate one point person, such as the CPO or other privacy professional, as the lead for the project, with the understanding that all applicable stakeholders will continue to do their part as well to update and maintain the inventory. Some organizations opt to keep a long-term arrangement with a consultancy, having one or two consultants providing full- or part-time assistance beyond the initial data inventory process implementation.

STRATEGIC MISSION AND PROGRAM MISSION STATEMENT

Given the various data stakeholders and their different roles regarding company data, a company's data governance program will benefit substantially from the adoption of a company-wide policy that explains how data is to be treated in order to meet the company's overall strategic business goals. This will articulate the company's organizational objectives and values and inform employees and contractors how company data is generally to be collected, processed, used, shared, transferred, updated, retained, destroyed and made available to data subjects, employees, contractors, and others.

Considerations in developing an overall strategic policy include:

- What kinds of data the company collects and maintains, its purposes, and the related degrees of sensitivity;
- What legal obligations apply to company data;
- What industry self-regulatory obligations apply to company data;
- How the company may use various types of data, including to whom such data may be sold, shared or otherwise disclosed;
- Approaches to data governance by, and risk profiles of, peer companies;
- The company's risk profile, including the degree to which the company needs or desires to be privacy-protective and/or maintain industry-leading data security to protect its brand and customer relationships.

Some companies may wish to merely comply with applicable legal and industry self-regulatory obligations and contractual and other third-party commitments (which may include obligations imposed by insurers, customers, "Big Tech" vendors or even more routine service providers such as credit card companies), while others may seek to establish best practices and use that as a market differentiator. It used to be that companies operating only in the U.S. would have differing, usually lower, legal obligations than those with international operations, especially where European or similar laws apply. That is quickly changing as transparency and choice obligations become more and more heightened under U.S. privacy laws, particularly as it relates to more invasive types of processing (e.g., interest-based advertising). Moreover, as Big Tech vendors like Apple impose consent requirements for "tracking," EU-style consent is becoming a global requirement in certain contexts. In the U.S., companies in industry sectors that have heightened data protection regulatory schemes, such as financial services and health care are often exempt from comprehensive privacy regulation (including the CCPA, CPRA, and CDPA); however, the exemptions only partly exclude compliance obligations for some organizations. As a result, those organizations may be required to comply with the sector-specific laws as to certain types of data and general privacy laws with respect to other types of data.

There will be a multitude of company policies and notices that will reflect the company's overall privacy practices and policies, including consumer privacy notices (including website and specific product privacy notices, and notices at collection), employee/contractor computer use (including "Bring Your Own Device") and social media policies, , a written information security policy (WISP), a data security breach preparedness and response plan, a policy of requiring privacy impact assessments for new or changed data practices or events, and others. This second level of policies all should reflect the companies' overall strategic data protection policy.

DEVELOPING AND IMPLEMENTING A PROGRAM FRAMEWORK

Developing a program framework will help in the articulation of the broad umbrella policy and its implementation through more specific polices and notices. Part of the framework is the governance structure. From the program stakeholder group comes the second level of governance - policies, procedures, processes, guidance documents, educational programs, compliance and request reporting mechanisms, guidance documents and checklists, and incident response plans that will enable policy implementation and compliance. Some aspects of the framework will be company-wide and some specific to products, services or functions. Having the input and participation of all stakeholders in program governance will help ensure effective implementation and ongoing assessment and refinement, which in turn helps reduce the risk data leakage or misuse that could cause economic and/or reputational harm to the company.

A program framework can be developed from applicable established standards. In many cases, organizations will have to apply a number of standards to the same data sets, including those required by law, self-regulation, or contractual or other third-party requirements. In many cases, an organization will want to apply a common standard, if possible, to all data, such as a “least common denominator” approach where the strictest standard is followed. In some ways, this may not be possible to remain compliant with all the standards; for example, the CPRA and CDPA include differing obligations and applying the “stricter” standard from one of the laws will not necessarily result in compliance with the other. And, as mentioned above, certain organizations may be required to comply with the sector-specific laws as to certain types of data and general privacy laws with respect to other types of data. In that case, it would not make sense to apply HIPAA-level security and other standards to non-health data, for a number of reasons, including cost, lost business opportunity, and others.

In addition, a number of helpful and instructive data protection standards have been set by standards organizations, such as the American Institute of CPAs’ Generally Accepted Privacy Principles and the International Organization for Standardization (ISO) 27000 series of information security standards. Public companies should also develop data protection frameworks, keeping their obligation under Section 404 of Sarbanes Oxley (requiring management and external auditor reports on the adequacy of the company’s internal controls on financial reporting) firmly in mind.

There are also best practices for privacy and data security that are recommended by the Federal Trade Commission and the California and other states’ Attorney Generals, and the concept of Privacy by Design (PbD), which has been adopted in various forms as either required or recommended by various data protection authorities worldwide.

PRIVACY BY DESIGN

Privacy by Design is the concept of operating and processing data pursuant to a company’s defined standards. PbD was pioneered in the 1990s by Ontario Canada Privacy Commissioner Ann Cavoukian. This much refined and time-tested approach has been recommended by the FTC in many of its privacy and data security guidance and policy documents and is essentially codified in the EU’s GDPR and now the CPRA and CDPA. In its true form, privacy is the default and products and services should be developed from conceptualization through exploitation to minimize privacy and data security impact and maximize consumer privacy, control and safety. Even if a company’s policy is not consumer friendly, and it operates only in jurisdictions like the United Sates - and there in minimally regulated industry where acceptable - the process of evaluating privacy and data security impacts all stages of product and services development and exploitation, rather than as an afterthought, has great value and helps avoids unnecessary inefficiencies and risks and costly last-minute workarounds. Below are the 7 linchpins of a successful PbD framework:

1. **Proactive not Reactive; Preventative not Remedial**. PbD does not wait for privacy risks (e.g., non-compliance) to materialize. It aims to prevent them from occurring. Stakeholders proposing new or different data processing activities go through proper channels to vet the new processing

activities to ensure review by other stakeholders (such as privacy, legal, and information security) in the company's privacy impact assessment procedures.

2. **Privacy as the Default Setting**. Personal data is protected automatically in any given IT system or business practice, without any action being required on the part of the data subject to do so.

3. **Privacy Embedded Into Design**. PbD is embedded into the design and architecture of IT systems and business practices. For example, a new vendor's data processing is considered across the board – such as how the vendor will be able to delete the company's data in response to a data subject request, or what level of security the vendor will be able to provide relative to the company's requirements/standards – when vetting the vendor initially and onboarding it at a later stage.

4. **Full Functionality – Positive-Sum**. PbD avoids the debate and trade-offs that meeting one standard requires diminution of another – e.g., privacy vs. security – and demonstrates that it is possible to avoid both.

5. **Full Lifecycle Protection of Data**. Strong security measures are applied to data throughout the retention period, and data is securely disposed at the end of the applicable processing.

6. **Visibility and Transparency**. A functioning PbD framework provides ways for various stakeholders to ensure that the business practices and IT systems are operating according to the stated promises, objectives, and standards.

7. **User-Centric Mindset**. The interests of data subjects/users are respected by providing strong privacy defaults and appropriate transparency and choice.

ESTABLISHING GOALS AND MEASURING PERFORMANCE

Once policies have been established and the program has begun to be implemented, the organization should set measurable goals to gauge program performance. Tracking and benchmarking indicators of program performance and maturity can help establish what is working and where improvements are necessary. In doing so, it is important to select enough relevant metrics and ensure they are objectively measured and accurately reported. Relevant metrics include: adequacy of notice at collection; consistency of access and use with policy; conformity with retention/destruction policies; results of security assessments; use of privacy impact assessments; employee policy knowledge; and number and severity of incidents and response time and effectiveness.

ASSESSING, PROTECTING, SUSTAINING AND RESPONDING

The operational functions of a data management program are often categorized by the literature on the subject as assessing, protecting, sustaining, and responding, and are applied across an operational lifecycle. The four phases represent key tasks, and lifecycle means not birth, growth, death and rebirth in the ecological sense, but that there is a process of constant evaluation and refinement as opposed to a one-time assessment and fix. Good programs are intended to continuously evolve and improve.

1. Assessing

Assessment is a critical initial step to new program creation (as well as crucial to existing program evaluation), to the evaluation of the impact of each new product and service, and of changes in facts, law or practices. In addition, risk assessments are codified into law by the CPRA and the CDPA for certain types of riskier processing. Assessment enables the company to understand its corporate goals, legal obligations, and the facts regarding data and data practices. It also enables the company to identify and fill in gaps, evaluate program success and failings, and establish return on investment data. All areas of a company that touch data, and all of the company's data stakeholders, need ongoing assessment. This can be institutionalized through the adoption of various assessment models and tools, including software tools, physical inspections, surveys and questionnaires, internal and third-party audits, impact assessment forms, and other fact-marshalling devices that provide input necessary for a meaningful analysis. Essentially, fact gathering by use of these tools is the monitoring function, and assessment is the analysis and conclusions and recommendations that come from monitoring activities.

There are well developed models for assessing overall program development. One is the now 20-year tested AICPA Privacy Maturity Model. It uses benchmarks to rate activities and programs to five maturity levels: *ad hoc*, repeatable, defined, managed and optimized. The AICPA offers an affordable software tool called the Privacy Principles Scoreboard that companies and their advisors can use to conduct privacy risk and maturity assessments. Two real values of engaging in such an exercise are that it helps track growth and success and can also be used as an objective measure of return on investment.

It is worth noting that Privacy by Design, as discussed above, is an assessment model for operating a data governance program (rather than rating one).

2. Protecting

Returning to the life cycle metaphor, protection of data can also be seen in this manner, and Data Life Cycle Management (DLM) is a common information governance approach to tracking and managing data from creation to destruction. DLM is concerned with how data is handled, retained, processed, stored, shared and destroyed. Data retention policies are important to comply with legal requirements, and to minimize risk associated with data retention beyond what is necessary or beneficial. Both privacy compliance and data security are also crucial to data protection throughout the data life cycle. As previously explained, although different requirements and frameworks may apply depending on the company and its data, established frameworks that may not be legally required are nonetheless good standards to draw from.

3. Sustaining

Sustainment is essentially about evaluating, enforcing, refining and educating. This flows out of monitoring and assessment. To sustain a program, monitoring and assessment needs to be ongoing. Compliance-monitoring, which requires systems to solicit, respond to, track and learn from complaints and mistakes, is an excellent way to sustain program goals. Indeed, part of sustainment is accountability. There should be trusted people and mechanisms for making complaints, requests, recommendations and whistle blowing. There also needs to be procedures for responding to and resolving issues and repercussions for non-compliance. Finally, employee and vendor training are essential. Anyone that touches, or has access to, company data or data systems needs some level of data protection sensitivity, which can only be had through ongoing education. Education is more than merely promulgating operational practices policies; it also includes educating people about the issues, why they are important, and how they relate to their particular role in the company and their daily activities. Some education is of a general nature and relevant to all, while other training should be function-specific and tailored to the relevant audiences.

4. Responding

In order to respond, there must be knowledge of an issue in need of response. The first three elements assist in this regard. Data protection programs need to be designed to respond to requests, inquiries, compliance failures, security breaches, disasters and other business interruption. There should be preparedness plans and systems in place for all. Also, companies should consider various cyber-liability and business interruption insurance policies to help mitigate the costs of inevitable issues.

Key to the ability to respond is preparedness, which is not only having well-conceived plans and procedures, but practical exercise to build the experience necessary to respond effectively when the time comes. This can be done through table-top exercises, which put response team members through likely scenarios, including internal and external breaches and natural and man-made disasters. In this regard, data protection incident response is similar in many respects to a good business continuity and disaster response plan, and indeed is a component of such planning. Furthermore, state laws and federal and state health care information laws may require data security incidents to be reported to regulators, data subjects and the public. These laws are far from consistent and may result in different obligations from state-to-state under identical facts, so having the ability to expeditiously address those requirements in the event of an incident, typically through outside legal counsel, is part of response preparedness.

CONCLUSION

In today’s digital age, all companies have data assets and obligations. Legal, privacy, IT/IS, and compliance leaders need to work together with other data stakeholders, within a defined and accountable governance structure, to develop a robust program for assessing that data and its corresponding obligations, protecting the data and evaluating and minimizing data-related risks. A good data management and protection program should necessarily incorporate Privacy by Design principles and be in a constant state of self-evaluation and improvement.