Deloitte.

Data privacy as a strategic priority

Enabling growth and innovation by using information governance to effectively manage data privacy risk

Introduction

In a world where the value and volume of data are growing exponentially, data privacy has emerged as a board-level issue and potential source of competitive advantage—not just a compliance requirement. But the devil is in the details. Without a comprehensive and effective program for information governance (IG), data privacy remains a compliance challenge and a potential reputation time bomb.

Companies today face increasing pressure from regulators and the marketplace to improve how they collect, use, store and delete personal information (PI), and how they manage data privacy. And the pressure will only increase as innovations such as the Internet of Things (IoT), mobile, and big data—as well as always-on virtual assistants—generate more and more data and insights about everything people say and do. Under certain circumstances, consumers now have the right to access and delete their data, and they can opt out of sale of their PI, further driving the need for strong information governance and management.

Until now, many companies' data privacy efforts have revolved around the specific privacy-related regulations and requirements for their industries, to which the standard response was a mix of narrowly-focused initiatives designed to satisfy those specific requirements without comprehensively tackling larger problems. However, that scattered, one-off approach to data privacy may no longer be good enough.

Driven by the rising importance and visibility of the data privacy issue—as well as by sweeping data regulations such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)—companies can benefit from a more comprehensive and coordinated approach to IG. Such an approach helps a business efficiently and effectively tackle the full range of data-related challenges—including data privacy. It does so by reconciling and rationalizing the overlapping and conflicting regulatory requirements and then addressing them in a coordinated manner that avoids duplication and gaps. It can also help the business use its superior data privacy capabilities as a strategic differentiator in an increasingly digital and competitive marketplace.

Regulatory compliance and beyond

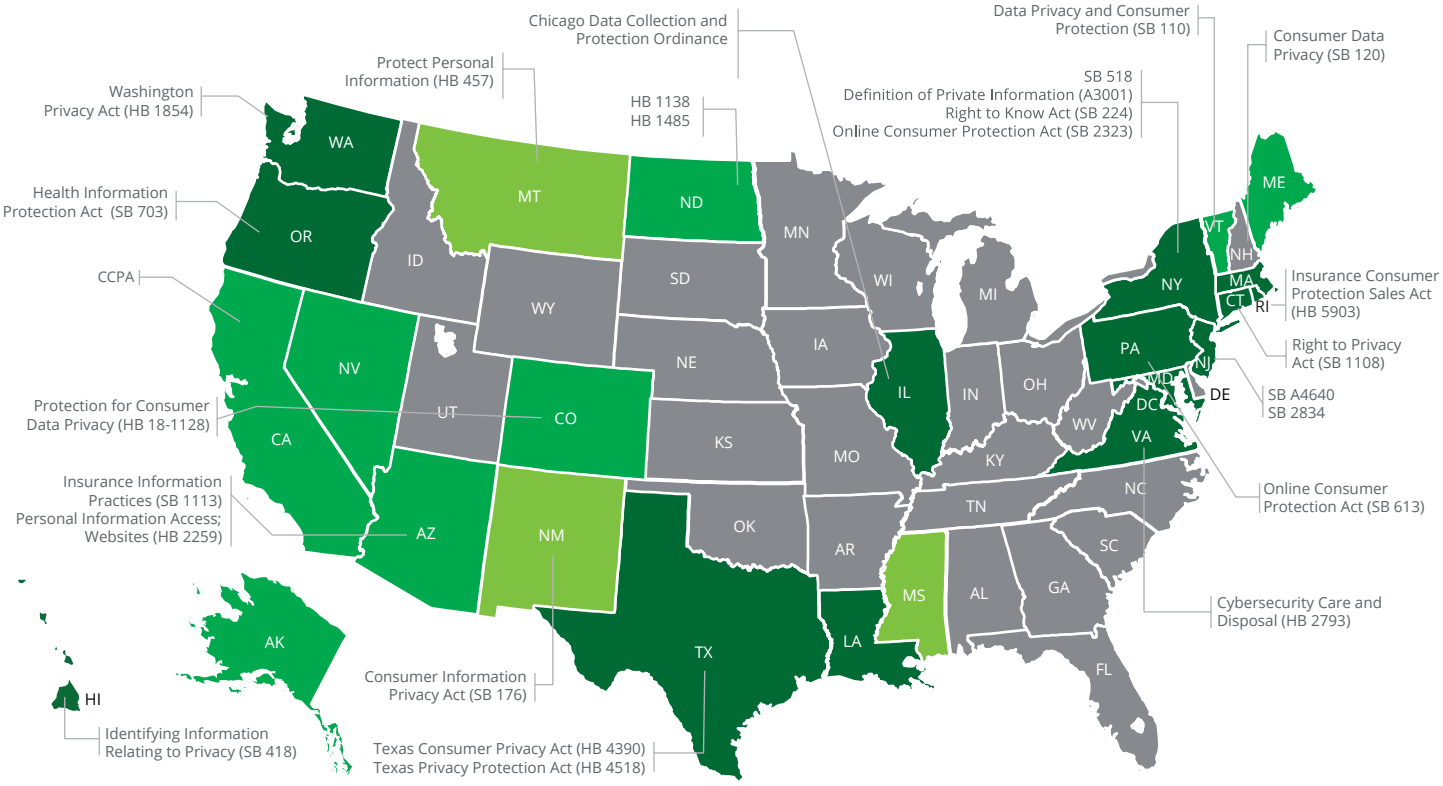
Regulatory requirements and business drivers are prompting companies to focus more attention and resources on managing data privacy risk:

- **Regulatory requirements:** Data privacy and cybersecurity rules not only require the protection of customer data, they impose obligations to assure the data's quality, completeness, and governance—including limited acquisition and use, as well as appropriate retention and disposition. Today, a number of states are considering legislation similar to the CCPA (Figure 1). These regulations span every aspect of a company's interactions with its customers.

- **Business drivers:** Companies are seeking competitive advantages in the marketplace by better mining existing information and taking advantage of non-traditional sources and uses of data, advanced analytics, artificial intelligence, and new ways of interacting with customers, such as digitization.

A comprehensive and coordinated IG program can enable companies to more effectively address both the regulatory requirements and the business drivers.

Figure 1: Similar legislative initiative to the CCPA[1]



These require more than just tougher information security; they require a comprehensive and effective IG program—along with the infrastructure necessary to collect only the required information and to retain it no longer than necessary. For example, section 500.13 of the New York Department of Financial Services (NY DFS) Cybersecurity Regulation states that companies "shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information that is no longer necessary for business operations or other legitimate business purposes, except where such information is required to be retained by law or regulation." (See sidebar on data minimization).

Data minimization: More isn't always better

One consequence of the complex and expanding set of data-related regulations is that many companies have begun to rethink their traditional posture of "keeping everything." They're taking steps instead to determine what information is needed, how it's protected and used, and how long to keep it. This emerging focus on data minimization is quickly rising to the top of the IG agenda, driven in significant respect by regulations including the GDPR and NY DFS Cybersecurity Regulations.

Until recently, the prevailing mindset about data was "more is better." But companies and regulators are now recognizing that it's possible to have too much of a good thing. Like a cluttered garage, collecting and retaining too much data creates a whole host of problems, including:

- **Cost**: The more data you have, the more it costs to store it.
- **Security**: The more data you have, the harder it is to secure—and the greater the potential risk of a security breach.
- **Reduced effectiveness**: When you have too much data, it's harder to find what you actually need.
- **Compliance**: The traditional "keep everything" approach now violates some of the new and emerging data regulations.

Companies need to actively determine what information to collect and keep, and how long to keep it. This will require careful analysis and reconciliation of the various regulatory requirements—many of which are overlapping or conflicting—as well as careful consideration of the company's information needs. It will also require new policies and system capabilities, including data-driven disposition and retention, that can help the company efficiently and effectively handle the day-to-day task of data minimization without losing valuable information or causing unnecessary risk.

Are your data privacy capabilities up to the task?

Thoughtful questions about the state of data privacy risk at your organization can help start the conversation and drive toward the right answers. Here are some key questions your organization should be asking:

- Are we being proactive in identifying and complying with all the laws and regulations that govern data capture, use, retention, security, and disposal at our company?
- Do we have an adequate information governance foundation in place that allows us to deal with current and upcoming data privacy challenges, such as consumer access and deletion requests, and consumers opting out of sale?
- Do we know what information we have, how complete and accurate it is, where it is, and how it's used and protected?
- Do we have the appropriate leadership, structure, capabilities, resources, and support to address these risks comprehensively—in the context of our business model and goals?
- Do we receive and retain the necessary information to support key business decisions and actions?
- Have we organized the compliance and privacy functions to best support and oversee our business and operations?
- How do our IG program and capabilities align to industry standards and peer organizations?

Key process areas for managing data privacy risks

Complying with the regulations can be difficult and complex, requiring companies to assess a wide range of activities (strategy, people, process, and technology), and to build diverse capabilities and tools in four key process areas (records management, privacy/compliance, crisis management/cyber, and IG). These capabilities and tools encompass:

- **Data inventory**: Companies need to know the type and source of data collected, stored, and used—and how accurate and complete it is. Inventories should be risk-ranked to reflect inherent risk and quantify business needs for the data.
- **Classification**: Companies need to define the types of data collected and retained—and which data is personal versus public—in a manner that's compliant with privacy regulations and that clearly classifies individuals impacted by the information to ensure customer access requests are properly addressed.
- **Third-party relationships**: Companies need a comprehensive inventory of third-party relationships (and of the data collected, stored, or shared with third parties) to implement programs that properly address issues related to data quality, use, privacy, and security. Contracts should be created or amended to hold these third parties to new privacy standards.

- **Portability and erasure**: Companies must manage customer requests that involve moving or eliminating personal information.
- **Data security**: Companies need to implement and maintain reasonable security procedures and practices. They also need to respond effectively to data breaches.
- **Consent**: Companies need management tools capable of handling consumer requests in a timely manner, including specific authentication and permissions for cross-affiliate marketing.
- **Oversight and monitoring**: Companies must implement programs that are comprehensive and strong, yet flexible enough to adapt to continued changes and ongoing regulatory/business implementations. Such programs can benefit from increased focus on training and change management procedures to ensure they're properly implemented through the three lines of defense, which can help avoid regulatory enforcement, fines, and penalties.

Data privacy and reputation risk

The increased number of laws and regulations is the vanguard of a paradigm shift in which the general population is growing more concerned about their private data. Recent headlines have shone a spotlight on the potential misuse of consumer data, and the reality is that any organization collecting data about consumers—especially if they share the data with vendors or third parties—may be at risk of having their data misused. Significant reputation damage can result from misused data and/or data breaches. Organizations should understand and prepare for the reputational risks that extend beyond non-compliance with the myriad of data privacy laws and regulations.

The three lines of defense

In designing and implementing their approaches to IG, companies should assign accountability using the three lines of defense model.

To advance the effectiveness of this model, some organizations are placing the privacy function and its resources squarely within the compliance organization. After all, data privacy represents a critical, if not one of the most critical, compliance risk for these organizations. And tying the privacy and compliance functions together promotes oversight, clarity of roles and responsibilities, effective management of regulatory matters and relationships, and timely reporting to senior leaders and the board.

Figure 2: Typical roles and responsibilities across the lines of defense in privacy organizations

1st line of defense

Lines of business/privacy liaisons

- Owns privacy risks and overall accountability for protecting personal data against current and emerging risks across the data lifecycle
- **Operationalizes control procedures** to effectively align with privacy policies and applicable laws and regulations
- **Implements privacy** program within the lines of business
- Conducts **periodic assessments** to assess effectiveness of privacy controls
- Tracks and reports performance of privacy controls

2nd line of defense

Global privacy office & compliance

- Establishes **governance, policies, oversight, and accountability** for privacy
- Develops core **privacy program components** such as processes, tools, templates, guidance, and privacy notices for the lines of business to use in building controls
- Establishes **privacy risk assessment requirements** and performs second line risk-based monitoring and enforcement of privacy controls to ensure compliance
- Develops and implements competency-based training and awareness for privacy related policies and standards
- **Reports performance** of privacy program to the board; risk committees; and privacy, security, and data governance councils
- Manages **communication with supervisory authorities/regulators** on privacy and data protection

3rd line of defense

Internal audit

- Evaluates, on **an independent basis**, the effectiveness of privacy controls to provide assurance
- Regularly **reports control effectveness results** and challenges to senior leader and the audit committee

Practical lessons learned

Implementing a comprehensive and coordinated approach to IG can be challenging and time-consuming. Here are some leading practices to keep in mind:

- **Establish an enterprise governance strategy**: Create the vision, driven by executive leadership, to help ensure the program's success. Verify that the governance strategy supports and aligns with corporate strategy and growth objectives. Make sure line-of-business and functional leadership approves and supports the program prior to execution.

- **Deliver value quickly**: Ensure information assets deliver business value. Set realistic goals and expectations with program leadership. Maintain a straightforward, no-nonsense approach; simplicity is usually better. Measure success at the appropriate stages to confirm program alignment.

- **Build a foundation with the end in mind**: Establish an extendable IG model to support expanding business needs. The IG operating model framework should be able to support multiple types of data and customer interactions, and it must bring together all the relevant stakeholders.

- **Don't boil the ocean**: Perform sufficient due diligence during the planning phase to isolate and prioritize the top data issues/risks. Focus on determining the most cost-effective solutions and develop a comprehensive plan for resolution. Ensure solutions don't negatively affect customer-facing processes but improve them.

- **Establish business ownership and accountability for data**: Develop clearly defined roles and responsibilities and drive process improvements to gain efficiencies with lines of business and functional areas. Establish ownership within business management and mandate accountability for data quality.

- **Treat information governance as a program, not a project**: IG is a journey, and adoption must be institutionalized in the organization's culture. IG requires executive sponsorship and support to be effective; a bottom-up approach won't work. Policies and standards will need to be approved by the IG governance structure, and resources will need to be made available to test adherence and measure quality.

Getting started

Although the task of organizing and implementing IG can seem daunting, the end results are worth the attention and effort. In addition to enabling compliance with data privacy regulations, IG can pay significant business dividends—particularly when accomplished through careful planning and execution, collaboration with all key stakeholders, and strong executive sponsorship. Here are some considerations for getting started:

- Assess the current state of IG capabilities across the enterprise
- Develop a vision for IG tailored to the organization's data privacy risks and requirements, as well as its business strategy and goals
- Craft a multiyear roadmap, with priority on high-impact initiatives
- Develop, fund, staff, and roll out the IG program organization
- Select and begin to implement IG tools
- Consider an experiment or pilot to understand value and opportunity

Ultimately, the path to effective management of data privacy risk through IG starts by making it a high priority within your organization. Are you ready to take that critical first step?

Endnotes

1. Sources for CCPA similar initiatives: https://adexchanger.com/privacy/bevy-of-ccpa-amendments-pass-california-assembly-next-stop-the-senate/
https://iapp.org/news/a/ccpa-update-senate-committee-pares-back-amendments/
https://www.dataprotectionreport.com/2019/06/nevada-new-york-and-other-states-follow-californias-ccpa/
https://www.lexology.com/library/detail.aspx?g=b9b1a955-c0e4-4f65-a33b-e7af82224477
https://www.cyberadviserblog.com/wp-content/uploads/sites/18/2019/06/State-Privacy-Law-Tracker-06-19.pdf

Contacts

Jay Cohen
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
jaycohen@deloitte.com

Tim Cercelle
Managing director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
tcercelle@deloitte.com

Rich Vestuto
Managing director
Deloitte Risk & Financial Advisory
Deloitte Transactions and
Business Analytics LLP
rvestuto@deloitte.com

Niels Aafjes
Senior manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
niaafjes@deloitte.com

Deloitte.