CADENCE GROUP

acquire > organize > disseminate

# The U.S. Data Privacy Landscape and the Case for Information Governance

**In this paper you will learn:**

- ✓ Recent developments in the U.S. privacy landscape
- ✓ The scope and business obligations under the Virginia Consumer Data Protection Act
- ✓ Ways to prepare for the "new" privacy-regulated environment
- ✓ How to assess your organization's data privacy and information governance maturity; and
- ✓ Why implementing an Information Governance framework is an important step in building a sustainable compliance program

## Table of Contents

## The U.S. Privacy Landscape and a Survey of State Privacy Legislation

Have we reached a new compliance era? Although a comprehensive federal privacy law has not been enacted by the United States comparable to Europe's Generation Data Protection Regulation (GDPR), multiple states are taking action to ensure that (consumer) data is protected. As we discussed in an earlier post, California was the first state to enact a comprehensive state privacy law. Now a second state has signed into law a wide–ranging privacy act similar to the California Consumer Privacy Act (CCPA). On March 2, 2021, the Virginia Consumer Data Protection Act (VCDPA) became law. Several other states are poised to pass similar legislation this year. Let's review Virginia's CDPA and survey the progress of other state privacy legislation.

### Background and Context of VCDPA

Many people have now heard of the California Consumer Privacy Act or CCPA, which was enacted in 2018. In 2021, California overhauled its privacy framework again by voting in favor of Proposition 24, known as the California Privacy Rights Act (CPRA), which concurrently strengthens and weakens CCPA. Most importatly, it expands CCPA's range, and enhances consumer privacy protections outlined in CCPA by clarifying rights and imposing additional obligations on businesses (subject to the CPRA's provisions). CPRA, which becomes effective January 1, 2023, is intended to eventually replace the CCPA, but not immediately. (The scope of this article goes beyond California's complex legal framework and it's implementation. Seek out advice from your general counsel for specifics).

The Virginia Consumer Data Protection Act (CDPA) became law in March 2021 and is enforceable starting January 1, 2023. Its substance is comparable to other privacy laws (i.e. proposed Washington Privacy Act and the California Consumer Privacy Act); however, in a few key aspects this legislation is more consistent with GDPR, most notably its:

- Requirements for data protection assessments
- Use of the terms "controller" and "processor" to describe businesses and service providers that possess or manage protected data; and
- Establishment of an enforcement authority; in this case, the VA Office of the Attorney General

Both Virginia's CDPA and California's CPRA impose risk assessments on companies to determine how the processing of sensitive personal information could pose risks to the rights of consumers. The VCDPA requires companies to conduct a Data Protection Assessment (DPA) when

(i) personal data is sold,
(ii) personal data is used for targeted advertising,

(iii) processing of personal data for profiling could create a foreseeable risk of harm to consumers,
(iv) sensitive information is processed or
(v) processing could otherwise pose a heightened risk of harm to consumers.

Furthermore, the DPA must identify and weigh the direct and indirect benefits from the processing of the information to the business, consumer, other stakeholders, and the public against the potential risks to the consumer's rights. A key difference, though, is that CPRA also stipulates that a company submit a risk assessment "on a regular basis" to the California Privacy Protection Agency and perform a cybersecurity audit on an annual basis, while VCDPA does not.

## What is the Scope of VCDPA?

Generally, the most important consideration when a new law is passed is: Does it apply to my organization? VCDPA will most likely apply to for-profit and business-to-business companies interacting with Virignia residents, or processing personal data of Virginia residents on a relatively large scale. More specifically, this law compels certain obligations on entities that conduct business in Virginia or produce products and services that are targeted to Virgnia residents, during a calendar year, which either:

- Control or process data of at least 100,000 consumers, or
- Control or process data of at least 25,000 consumers and derive 50 percent of gross revenue from the sale of personal data.

The statute broadly defines personal data as "any information that is linked or reasonably linkable to an identified or identifiable natural person[,]" and to exclude "de-identified data or publicly available information." It defines "sensitive information" as data that includes:

- "Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
- The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
- The personal data collected from a known child; or
- Precise geolocation data."

Also of note: the definition of 'consumer' as any "natural person who is a resident of the Commonwealth *acting only in an individual or household context*" is important. VCDPA provides consumers with several rights. The first three provide consumers the right to access, correct, and delete their personal information. Other rights that are outlined in the legislation are:

- Right to receive notice of processing activities

- Right to data portability (i.e. data must be in a readily usable format, so it can be transferred from one entity/platform to another)
- Right to opt out of behavioral advertising
- Right to object to automated profiling and decision making
- Right to non-discrimination for the exercise of these rights
- Right to opt out of sales of personal information

Furthermore, controllers must establish and describe a secure process for which consumers can exercise such rights. What is exempted, however, pertains to data when an individual is "acting in a commercial or employment context."

## What are the Exemptions and Business Obligations outlined in CDPA?

The law outlines two main types of exemptions: entity-level and data-level exemptions. The entity-level exemptions are:

1. A body, authority, board, bureau, commission, district, or Virginian agency or any Virginian political subdivision.
2. Any financial institution or data subject to the Gramm-Leach-Bliley Act.
3. A covered entity or business subject to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).
4. A nonprofit organization.
5. An institution of higher education.

## Key Business Obligations required under the VCDPA

Now that we have a baseline for whether the law applies to one's organization, let's review key business obligations:

1. Businesses are limited on the collection and use of data, and will be required to implement certain technical safeguards. Specifically, the law requires businesses to "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect confidentiality, integrity, and accessibility of personal data" (S.B. 1392 § 59.1-574(A)(3).
2. Controllers must conduct formal "data protection assessments" for certain types of data that they collect. There is no prescription, however, for how frequently the assessments need to be conducted.
3. A contract between a controller and processor must be created to govern the processor's data processing procedures (and outlining the controller's instructions, the nature and purpose of processing, and the obligations of each party, and duties of confidentiality).

4. Businesses that process "sensitive data" will be required to obtain consumer consent for such processing.

## Besides CA and VA, What Other states have Passed Privacy Legislation?

A handful of other states have passed their own data privacy laws; however, they are not as comprehensive as California and Virginia's laws. One of these is New York's Stop Hacks and Electronic Data Security ("SHIELD") Act, which also specifies that businesses implement reasonable security measures to protect personal information and became effective March 21, 2020.

Another notable data privacy law is the Nevada Privacy of Information Collected on the Internet from Consumers Act, which applies to operators of commercial websites and online services. Its scope resembles the California Online Privacy Protection Act, but is actually much narrower. The Nevada law imposes obligations on these entities that collect and maintain "covered information", personally identifiable information (i.e. first and last name, email address), from consumers who reside in Nevada and use or visit the websites or online service; and engage in activities that establish an adequate nexus with the State.

While these laws vary greatly in substance and entities subject to the laws, both mandate that certain organizations address the collection and maintenance of personally identifiable information.

## U.S. State Privacy Comparison

In the absence of a federal policy, states are moving forward with their own data privacy legislation. As previously mentioned, the U.S. is at the proverbial tip of the data privacy iceberg, as more states have recently passed or are actively considering various forms of data privacy legislation. The International Association of Privacy Professionals (IAPP) approximates that 15 states have introduced bills that are still active in state legislatures. So, what common provisions do current and proposed data privacy laws have for consumers and what are the business obligations? According to IAPP, the state bills contain the following consumer rights:

- Right to access
- Right of rectification
- Right of deletion
- Right of portability
- Right of opt-out
- Right Against Automated Decision Making

IAPP has identifed some common business obligations as well:

- Opt-in requirement age

- Notice/transparency requirement
- Risk assessments
- Prohibition on discrimination (exercising rights)
- Purpose/processing limitation

## The Cost of Inaction

The business obligations discussed are only a general description of the types of regulations that states will likely impose on organizations in the coming months and years. The varying scope and increasingly frequent emergence of these laws present complex compliance challenges for non-exempt organizations. The two states with comprehensive data privacy legislation, California and Virginia, have divergent approaches to enforcing non-compliance.

- California's privacy legislation has a "Privacy Right of Action" provision, which provides California consumers with a private right of action when "[a]ny consumer whose non-encrypted and non-redacted personal information … is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information[.]" The California Privacy Rights Act (CCPRA), a ballot initiative that passed at the polls and amends CCPA, creates a new administrative agency to "implement and enforce" these new laws. The administrative agency will have several responsibilities, including the duty to promulgate, revise, and implement regulations interpreting the CCPA and CPRA by July 1, 2021 or six months after the CPPA indicates it is ready to begin rulemaking. Additionally, CCPA will have the authority to conduct its own hearings, subpoena witnesses and compel their testimony, take evidence, and impose fines upon any violators.
- Virginia's law does not have a privacy right of action provision for data breaches. The VCDPA is only enforceable through the Virginia Attorney General's office. When there is an alleged violation a business will have 30 days following the AG's notice to cure the alleged violation.

The potential fines for non-compliance make the need for compliance urgent. For example:

- In Virginia, when there is violation "in breach of an express written statement provided to the consumer[.]" the Attorney General's office can seek damages up to $7,500 for each violation.

- In California, fines in violation of the California Privacy Rights Act (CPRA) are up to $2,500 per violation and up to $7,500 per intentional violation or violation involving those under 16.

Organizations large and small would be well-advised to address information data privacy proactively as these bills make their way into law. The question is, where to start?

## How Should Companies Prepare for these New State Regulations?

Now that the U.S. privacy landscape has changed and other states are expected to pass their own legislation in the coming months, companies compliance. Experts recommend taking the following measures:

- Perform a new data mapping exercise to determine which elements of personal information they collect is "sensitive personal information";
- Evaluate their data retention policies internally;
- Update their privacy statements with newly required disclosures;
- Implement a mechanism for allowing consumers to request data correction; and
- Update their "Do Not Sell" mechanism to either include a second "Limit the Use of my Sensitive Personal Information" button, or bundle both mechanisms under one button.

## Getting Started: Assess Data Privacy and Information Governance Program Maturity

As mentioned above the CCPA (and CPRA) and VCDPA take effect on January 1, 2023. So it is incumbent upon organizations to prepare for these new state privacy regulations, including assessing their privacy risk. A privacy risk assessment produces the information that can help an organization compare the benefits of its data processing with the risks to determine the appropriate response.

Both state privacy laws require organizations to conduct data protection assessments. CCPA stipulates that organizations submit to the California Privacy Protection Agency a risk assessment on a regular basis and that it document if the processing involves sensitive personal information, and they must identify and compare the processing with the rights of the consumer; as well as determine if the risks outweigh the benefits. Although CCPA requires companies to conduct a risk assessment, and the VCDPA mandates both security and assessment requirements, they do not provide specific guidance on how to conduct a data protection/data assessment or how often it should be conducted. Note, Virginia's CDPA legislation specifies the types of data collection activities that must be assessed.

To assess data privacy, organizations are advised to create a compliance plan. IAPP has various resources (including European guidelines) on approaches to managing privacy

risk. Initially, an entity should outline precisely how it defines risk or, more specifically, build what the U.S. National Institute of Standards and Technology (NIST) refers to as a "Privacy Framework". This will be discussed in more detail below.

While current privacy regulations do not offer specific guidance and a universal risk assessment template does not exist, there are certain actions organizations can undertake to ensure compliance with their privacy obligations. After identifying privacy risk, the next step is to conduct a data protection impact assessment (DPIA). To be clear certain high risk business conditions warrant an immediate DPIA; however, with the new regulations soon to be effective, we suggest conducting a risk assessment that is designed to minimize your liability and ensure best practices for data security and privacy compliance. Data privacy best practices include:

- Approach data privacy universally. Consider data privacy as a holistic risk management issue for the organization.
- Map your data. Understand what you have, who owns it, who has access to it, where it's stored, and where it is shared – both inside and outside of the organization.
- Ensure your service providers and other data stakeholders have robust data policies and procedures that meet your standards. Ensure that these data privacy requirements are documented in your service level agreements.
- Review and update your practices regularly. What you collect and what you do with what you collect changes more often than you might think.
- Conduct ongoing training programs for staff on security, privacy threats and data protection best practices

In coordination with private and public stakeholders, NIST developed a voluntary tool, *"Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management"*, which can equip organizations with enhanced engineering practices and privacy protection methods. This privacy framework can support organizations in several ways, including ensuring compliance with data privacy obligations and "future proofing" products and services to meet the obligations. To be clear, it is not a data protection impact assessment, but it can help organizations with the question "How are we considering the impacts to individuals as we develop our systems, products, and services?" The NIST "Privacy Framework" also outlines mechanisms and approaches organizations can take to meet data privacy compliance obligations.

Identifying the regulations that affect your organization, conducting a privacy impact assessment and applying select elements of the NIST Privacy Framework are important foundational steps for your compliance program. However, these steps are only the beginning. Information compliance efforts must be built on a solid governance foundation. Policies and process must be aligned with business objectives, and consistent monitoring systems must be implemented to keep the compliance foundation strong. The framework that ties together risk management, privacy compliance, records and

information management, and technology systems to business objectives is called *Information Governance.*

## The Information Governance Assessment

ARMA International defines Information Governance as:

> *"…a strategic, cross-disciplinary framework comprised of standards, processes, roles, and metrics that hold organizations and individuals accountable for the proper handling of information assets. The framework helps organizations achieve business objectives, facilitates compliance with external requirements, and minimizes risk posed by substandard information-handling practices."*

The Information Governance (IG) framework is an often-overlooked component of a compliance program that can both minimize information risk and maximize informational value. The framework is built on 8 principles:

1. **Accountability**: There must be a chain of command with a senior executive leading the program.
2. **Transparency**: Policies, processes and procedures must be transparent.
3. **Integrity**: The information managed by the organization must be authentic and reliable.
4. **Protection**: The information governance program must provide appropriate protection to information assets.
5. **Compliance**: The information governance program must be designed to comply with internal requirements and external regulations.
6. **Availability**: Information must be made available for accurate and timely retrieval.
7. **Retention**: The organization must maintain records for a period of time that both meets operational requirements and complies with external regulations. *Retention, perhaps more than any other principle, is where data privacy compliance and records management need to be completely in sync.*
8. **Disposition**: Information must be disposed in a timely and secure manner.

But how does an organization measure the health and maturity of its information governance program? We at Cadence Group often use the Information Governance Maturity Model from ARMA International to assess program maturity for our clients. The Information Governance Maturity Model measures program maturity across the above 8 Principles and assigns a score from 1 (substandard) to 5 (transformational). The proper application of this maturity model will yield actionable goals that aid organizations in building and maintaining a *sustainably compliant* data privacy program.

## Need Help Getting Started?

Cadence Group's experienced team of information governance consultants can assist your organization navigate the tricky world of privacy regulations and get you on the road to compliance. Our service offerings include:

- Information Governance Program Assessment (including maturity modeling)
- Records and Information Management Policy and Procedure Development
- Records Retention Scheduling (including privacy compliance)
- Information repository mapping and data cleanup
- Program audits

For more information, contact us or visit www.cadence-group.com.

## Summary

The privacy law landscape is rapidly changing; several state legislatures are on track to pass comprehensive-privacy legislation this year. Additionally, there is a heightened data risk with more employees working remotely in 2020 and 2021, all of which puts a premium on having a proactive and comprehensive data strategy. Assessing data privacy from an organizational perspective involves a holistic approach beginning with a compliance plan and applying data privacy best practices to your organization. Identify the regulations that affect your organization, conduct a privacy impact assessment, and apply select elements of the NIST Privacy Framework to initiate a sound compliance program. Follow up by instituting (or evaluating) a sound Information Governance program to be the framework that addresses and applies risk management, privacy compliance, records and information management, and technology systems to business objectives.

The IG framework minimizes information risk and maximizes informational value ensuring that your organization achieves its business objectives, and more. Organizations should re-evaluate their privacy and data security programs, and integrate them with Records and Information Management initiatives to holistically address information risk and implement protection measures to mitigate those risks. Additionally, they should work to develop a program that is flexible and responsive to change, as the privacy landscape is currently fluid and ever-evolving.

## About Cadence Group

Cadence Group, a certified woman owned small business, is a user-centric information management consulting firm with 30 years of experience in information management services. Headquartered in Atlanta, GA, with an office in Washington, D.C., Cadence Group provides services to corporate, non-profit, and government clients. By creating structured, compliant, and sustainable information management strategies for web and content management, records and information management, libraries, collaboration and

knowledge management, technical assistance and training, and information technology, Cadence Group helps clients easily acquire, organize, and disseminate information.

## Resources


International Association of Privacy Professionals https://iapp.org/

IAPP Template for Data Protection Impact Assessment (published by Family Links Network) https://iapp.org/media/pdf/resource_center/dpia-template.pdf

European Union Data Protection Impact Assessment guidance https://gdpr.eu/data-protection-impact-assessment-template/?cn-reloaded=1

Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

UK's Information Commissioner's Office sample DPIA template https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf

Microsoft – Data Protection Impact Assessment for the GDPR (geared towards MS products but has information on what is required to complete a DPIA) https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-data-protection-impact-assessments

ARMA International's Information Governance Maturity Model and Information Governance Body of Knowledge ("IGBOK"): https://www.arma.org/page/Information_Governance

The Association for Intelligent Information Management: www.aiim.org

The Information Governance Reference Model: https://edrm.net/resources/frameworks-and-standards/information-governance-reference-model/

Ahmed, H. (2020, March 18). Best Practices for Privacy Audits. ISACA. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-6/best-practices-for-privacy-audits

Ayala, et al. (2015). NIST Privacy Framework: A tool for improving privacy through enterprise risk management. National Information Standards Organization. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

Bahar et al. (2021). Virginia is for lovers (of privacy)- the Consumer Data Protection Act passes into law. Eversheds Sutherland. https://us.eversheds-sutherland.com/mobile/NewsCommentary/Legal-Alerts/240131/Virginia-is-for-lovers-of-privacyThe-Consumer-Data-Protection-Act-passes-into-law

Brumfield, C. (2020, December 28). 12 new state privacy and security laws explained: Is your business ready? CSO Online. https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html

Cole, C., Baker, M.R. & Burgess, K. (2020, November 16). Move Over, CCPA: The California Privacy Rights Act Gets the Spotlight Now. *U.S. Law Week*. https://news.bloomberglaw.com/us-law-week/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now

Hart, C. (2019, November 26). What is data privacy? Northeastern University. https://www.northeastern.edu/graduate/blog/what-is-data-privacy/

Jacobs et al. (2021, March 13). Saturday Seminar – how should the United States protect data. *The Regulatory Review*. https://www.theregreview.org/2021/03/13/saturday-seminar-how-should-united-states-protect-data/

Kessler, D., & Ross, S. (2021, March 8). Virginia's new Data Protection Act. Norton Rose Fulbright. https://www.dataprotectionreport.com/2021/03/virginias-new-consumer-data-protection-act/

Klar, R, & Rodrigo, C.M. (2021, February 10). New state privacy initiatives turn up heat on Congress. *The Hill*. https://thehill.com/policy/technology/538122-new-state-privacy-initiatives-turn-up-heat-on-congress

Ramos, G.A. & Darren, A. (2021, March 3). Virginia Enacts Comprehensive Data Privacy Legislation. *The National Review*. https://www.natlawreview.com/article/virginia-enacts-comprehensive-data-privacy-legislation

Reader, R. (2021, February 21). These states are on track to pass data privacy laws this year. *Fast Company.* https://www.fastcompany.com/90606571/state-data-privacy-laws-2021

Sweeney, Jr., P.W., & Clancy, T.C. (2021, January 13). California voters approve (another) overhaul of California consumer privacy rights act. *The National Review.* https://www.natlawreview.com/article/california-voters-approve-another-overhaul-california-consumer-privacy-laws-meet

Wolford, B. (2021). Data Protection Impact Assessment (DPIA). GDPR.eu. https://gdpr.eu/data-protection-impact-assessment-template/

California Consumer Privacy Act. (2021). Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

NY SHIELD Act and the Bevy of State Privacy Legislation to Come: Are You Prepared? (2021). Lexology. https://www.lexology.com/library/detail.aspx?g=dac509df-ab5f-4bb6-8e8d-d1535ab780ce

Privacy Risk Assessment. (2020, March 24). Ensighten. https://www.ensighten.com/blog/privacy-risk-assessment