Privacy Alert
March 2021

Va. Passes Comprehensive Data Privacy Law, Requires Opt-in For Sensitive Personal Data

Virginia has become the second state in the United States to pass a comprehensive data privacy law and the first with a law requiring opt-in consent to process sensitive personal information. More like the European Union's General Data Privacy Regulation (GDPR) than California's Consumer Privacy Act (CCPA), the Consumer Data Protection Act (CDPA) gives consumers several privacy rights and imposes several obligations on businesses.

The law, which will go into effect on Jan. 1, 2023, applies to all businesses that either 1) control or process the personal data of at least 100,000 consumers during the calendar year, or 2) derive more than 50% of gross revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers.

While Virginia may be the second state to enact a comprehensive privacy law, it likely won't be the last. Washington, New York, Florida, Utah and Ohio are among the many states considering privacy laws during this legislative term.

Key Takeaways

- The CDPA uses GDPR-like language, applying its requirements to "controllers" and "processors," requiring impact assessments for certain "risky" activities, and imposing principles of data minimization and purpose limitation on covered businesses.
- It is the first comprehensive U.S. privacy law to require opt-in consent for the use of sensitive personal information, which includes race, ethnicity, precise geolocation data and certain health data.
- The law goes beyond the CCPA, giving consumers the right to opt out of targeting, advertising and profiling with significant or legal effects, in addition to sales.

Scope

Thresholds

The CDPA applies to "persons" that conduct business in the commonwealth or produce products or services that are targeted to residents of the commonwealth, and that meet one of the following thresholds:

- Process or control data of at least 100,000 consumers during a calendar year
- Process or control data of at least 25,000 consumers and derive over 50% of gross revenue from selling personal data

All parties in scope (controllers, processors, third parties and affiliates) are subject to the law if they meet these thresholds.

Exemptions

The CDPA provides exemptions for certain businesses and certain categories of data. The following businesses are exempt from the CDPA:

- Financial institutions or data subject to the Gramm-Leach-Bliley Act (GLBA)

Attorney Advertising

- Covered entities or business associates governed by the Health Insurance Portability and Accountability Act (HIPAA)
- Nonprofit organizations
- Institutions of higher education

The following data is exempt:

- Protected health information under HIPAA (and health records under Virginia's health law)
- Patient-identifying information for purposes of 42 U.S.C. § 290dd-2
- Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46 (or that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines)
- Personal data used or shared in research conducted in accordance with applicable law
- Information that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA
- Personal information collected for use in a consumer report, and by a user of a consumer report under the Fair Credit Reporting Act (FCRA)
- Personal data covered by the Driver's Privacy Protection Act
- Personal data regulated by the Family Educational Rights and Privacy Act (FERPA)
- Personal data covered by the Farm Credit Act

Notably, employee and business data are exempt from the law as well.

Covered Data

The CDPA defines personal data as "any information that is linked or reasonably linked to an identifiable or identified natural person." De-identified data and publicly available information are excluded from this definition. Pseudonymous data is exempt from some of the consumer rights obligations—including the right to correct, delete and access—but is not entirely excluded from the definition of personal data.

Consumer Rights

The CDPA provides consumers with many rights that have become standard in comprehensive privacy laws, including the rights to access, correct and delete personal data. Consumers also have the right to confirm processing and to obtain portable copies of personal data. The CDPA goes beyond the CCPA and provides a right to opt out of targeted advertising and profiling with significant or legal effects, in addition to the right to opt out of a sale of personal data. The CDPA does not address authorized agents, nor does it explicitly require companies to honor browser-based opt-outs.

Consumers have the right to opt in to the processing of sensitive information. The standard for consent mirrors that of the GDPR: It must be a clear, affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to process personal data.

Under the CDPA, a sale is defined as an exchange of personal data for monetary consideration by the controller to a third party. The CDPA does not include the "other monetary value" language that has caused confusion in the CCPA. However, narrowing this definition is likely to have minimal impact, as the law also allows for opt-outs of the targeted advertising and profiling that often fall into the definition of data shared for "other valuable consideration."

The CDPA also explicitly excluded the following from the definition of "sale":

- The disclosure of personal data to a processor that processes the personal data on behalf of the controller
- The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer
- The disclosure or transfer of personal data to an affiliate of the controller
- The disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience
- The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the controller's assets

Business Obligations

The CDPA is much less prescriptive than the CCPA. Businesses are required to authenticate a consumer request, but the exact methods are not specified. Companies have 45 days (with a 45-day extension) to reply to a consumer request. Requests can be made up to twice per year free of charge. Controllers must establish a process through which consumers can appeal the denial of a request.

GDPR-Like Principles

Controllers must limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. Controllers cannot process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed.

No Discrimination

As with the CCPA and the California Privacy Rights Act (CPRA), controllers cannot deny goods or services, charge different prices or rates for goods or services, or provide a different level of quality of goods or services to consumers who exercise their rights under the law. That said, products/services that require consumer data and loyalty, rewards, premium features, discounts or club card programs are not considered discriminatory.

Risk Assessments

A controller must conduct and document a data protection assessment of each of the following processing activities involving personal data:

- The processing of personal data for targeted advertising
- The sale of personal data
- The processing of personal data for purposes of profiling, where profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injuries to consumers
- The processing of sensitive data
- Any processing activities involving personal data that present a heightened risk of harm to consumers

Impact on Vendor Relationships

Controllers and processors must have a written contract in place. As with the GDPR, the contract should set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of the processing, and both parties' rights and obligations.

The contract must also require the processor to:

- Ensure that each person processing personal data is subject to a duty of confidentiality
- At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law
- Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with its obligations
- Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor (the processor may arrange for a qualified and independent assessor to conduct an assessment)
- Engage any subcontractor under a written contract that requires the subcontractor to comply with the obligations imposed on the processor

Contracts drafted to meet the GDPR's requirements will likely satisfy these requirements.

Enforcement

The CDPA has no private right of action and will be enforced by the Office of the Virginia Attorney General, which can seek civil penalties after a 30-day opportunity to cure. Fines will be up to $7,500 per violation, and the attorney general may also seek an injunction for activities in violation of the law.

Related Professional

Jessica B. Lee . . . . . jblee@loeb.com

6596 REV1 03-05-2021