GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

March 2021

Virginia Enacts Comprehensive Data Privacy Legislation

On March 2, 2021, Virginia Gov. Ralph Northam signed the Virginia Consumer Data Protection Act (CDPA) into law, making Virginia the second state to have comprehensive data privacy legislation on the books. The CDPA is similar to the privacy regime enacted under the California Consumer Privacy Act (CCPA) and expanded under the California Privacy Rights Act (CPRA). Indeed, Virginia's CDPA and the CPRA will take effect on the same day, Jan. 1, 2023.

Non-Compliance Risk

While California's privacy law permits consumers to bring a private right of action for data breaches, Virginia's law is subject to enforcement only through the Virginia Attorney General's office, which can seek damages up to $7,500 for each violation "in breach of an express written statement provided to the consumer[.]" Under the CDPA, businesses will have 30 days to cure any alleged CDPA violation following the AG's notice of the alleged violation. If a controller or processor cures the violation and notifies the AG's office in an express written statement within the 30 days, affirming that no further violations will take place, no action for statutory damages will be initiated against the controller or processor. The statute does not discuss what occurs if a violation cannot be wholly cured, such as for a breach of personal information.

Scope and Application

The CDPA applies to businesses that "(i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) [] control or process personal data of at least 25,000 consumers ***and*** derive over 50 percent of gross revenue from the sale of personal data." *See* S.B. No. 1392 § 59.1-572 (emphasis added). The statute defines personal data broadly to include "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." Consumers are defined to include Virginia residents "acting only in an individual or household context[.]" The definition "does not include a natural person acting in a commercial or employment context." The statute utilizes EU General Data Protection Regulation (GDPR)-like language, referring to "controllers" and "processors" rather than California's "business" and "service provider" language, and explicitly subjects both controllers and processors to potential liability for violations.

The statute imposes certain affirmative obligations on controllers, such as data minimization, maintenance of reasonable security controls "appropriate to the nature and volume of data at issue," non-discrimination rights for consumers, and requirements to process sensitive data only with consumer consent. It also requires controllers to provide a "reasonably accessible, clear, and meaningful privacy notice" of its data collection practices, including if it sells personal information or uses such information for targeted advertising.

While both the CDPA and California's CPRA are enforceable starting Jan. 1, 2023, only the CPRA will create a 12-month lookback for access requests, meaning that a company must have proper retention protocols in place to satisfy CPRA access requests by Jan. 1, 2022. The CDPA also broadly exempts certain data from its purview, including exemptions for covered entities or business associates regulated under HIPAA and Hi-Tech, financial institutions and data subject to the Gramm-Leach-Bliley Act, data collected for credit reporting purposes under the Fair Credit Reporting Act, data regulated under other statutes such as the Driver's Privacy Protection Act of 1994, the Family Educational Rights and Privacy Act, the Farm Credit Act, and data processed or maintained in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party.

Individual Rights

The CDPA will provide the following consumer rights, which largely mirror those provided by the CPRA.

- Right to receive notice of processing activities.
- Right to access personal data.
- Right to data portability (i.e., data must be provided in a readily usable format, so it can be transferred from one entity/platform to another).
- Right to correct errors in personal data.
- Right to delete personal data.
- 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.

Whereas the CDPA does require that organizations "authenticate" consumer data requests, it does not provide guidance or a description of how such authentication should be accomplished.

Sale and Targeted Advertising

Notably, unlike California's privacy law, the CDPA defines "sale" more narrowly as an exchange of personal data for monetary consideration; California's "sale" definition includes transfers for *valuable consideration* as well as money. In this regard, the CDPA's sale definition more closely tracks Nevada's SB 220 privacy law than California's.

Virginia also allows consumers the right to opt out of the processing of personal data involving "targeted advertising," defined as displaying an ad based on the consumer's information derived from their activities "over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests." Although this exceeds the explicit language found in the CCPA and its implementing regulations, leading to certain ambiguity as to how to interpret the use of cookies and similar tracking technologies on a case-by-case basis in the digital advertising context, this definition largely aligns with the CPRA's "cross-context behavioral advertising" definition.

Data Protection Assessments – More Documentation

The CDPA 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 injury to the consumer, (iv) sensitive information is processed, or (v) processing could otherwise pose a heightened risk of harm to consumers. The DPA "shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks[,]" factoring in "[t]he use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed[.]" Disclosures of DPAs to the Virginia AG's office for civil investigations "shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment."

California's CPRA imposes a similar requirement that businesses processing information which "presents significant risk to consumers' privacy or security" must submit a risk assessment "on a regular basis" to the California Privacy Protection Agency and perform a cybersecurity audit on an annual basis. The risk assessment should address "whether the processing involves sensitive personal information, and identify[] and weigh[] the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with such processing[.]"

Security Provisions

From a security standpoint, the Virginia law also requires controllers to "establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data," in a manner "appropriate to the volume and nature of the personal data at issue.

Data Processing Agreements

Unlike the CCPA, the CDPA requires that a contract between a controller and processor exist to govern the processor's data processing procedures. In addition to setting forth the controller's instructions, the nature and purpose of processing, the type of data and duration of the processing, and the obligations of each party, the law also requires that such agreements include duties of confidentiality; deletion or return of all personal data at the controller's direction; processors' demonstration of compliance with the CDPA upon the controller's reasonable request; "reasonable assessments" of the processor by the controller or its designated auditor; and the flow-down of obligations to subcontractors pursuant to a written contract. These provisions will largely be familiar to organizations who utilize data processing agreements pursuant to Article 28 of the GDPR.

Sensitive Data Processing

Unlike California's privacy law, the CDPA will require companies that process "sensitive data" to obtain consumer consent for such processing. *See* S.B. No. 1392 § 59.1-574(A)(5). Sensitive data includes 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; personal data collected from a known child; or precise geolocation data. While the CPRA does not require consent to collect and process sensitive data, Virginia will permit consumers to limit the processing of sensitive data.

No Private Right of Action, and Other Items Included in CCPA/CPRA *Not* Included in VA's CDPA.

Although there is significant overlap between Virginia's CDPA and California's comprehensive privacy law, differences do exist. California's law includes the following provisions that are not in the CDPA:

1. Private Right of Action. As noted above, California consumers have a private right of action when "[a]ny consumer whose nonencrypted 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[.]"

2. Sensitive Information Opt-Out. The CPRA permits California residents to opt out of the processing of sensitive personal information.

3. Financial Incentive Disclosures. California requires companies that have financial incentive programs (i.e., rewards programs) to provide notice of the program.

Opt-in Required for Consumers Under 16

California requires that users age 13 to 16 (inclusive) must "opt in" rather than having an "opt out" of the sale or sharing of their personal information.

Click here to subscribe to Greenberg Traurig's Data Privacy Dish blog.

GT GreenbergTraurig

Authors

This GT Alert was prepared by:

- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Darren Abernethy | +1 415.655.1261 | abernethyd@gtlaw.com
- Michael C. Hoosier | +1 415.655.1276 | hoosierm@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.