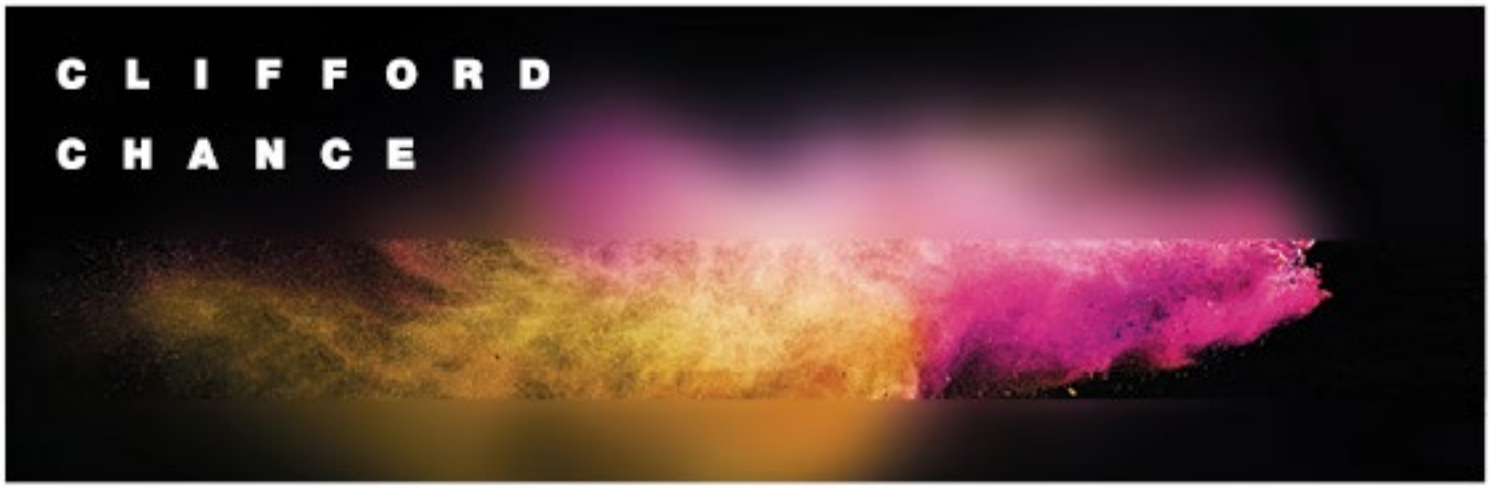

VIRGINIA'S CONSUMER DATA PRIVACY ACT

2021 is projected to be a pivotal year in privacy legislation and the year is off to a fast start. On March 2, the Commonwealth of Virginia became the first state to enact a comprehensive consumer privacy law in 2021. The Virginia Consumer Data Protection Act ("CDPA") draws heavily from the California Consumer Privacy Act ("CCPA") and the EU General Data Protection Regulation ("GDPR") and will impose significant new obligations on certain companies that process personal information of Virginia residents. The new law will go into effect in 2023.

Key issues

- Virginia became the first state in 2021 to enact a comprehensive consumer privacy law.
- The statute draws heavily from the CCPA and GDPR, but there are key differences companies should keep in mind as they update their compliance measures, such as strict consent requirements and special requirements for processing "sensitive" personal data.
- The Virginia Attorney General can seek civil damages of up to USD 7,500 per violation. However, companies can take solace in a 30-day cure period following notice of an alleged violation.
- The law does not provide for a private right of action.

OVERVIEW OF THE CDPA

Scope

The bill covers businesses in Virginia that target their products to Virginia residents and either:

- control or process personal data of at least 100,000 Virginia residents; or
- control or process personal data of at least 25,000 Virginia residents and derive over 50 percent of gross revenue from the sale of personal data.

Notably the CDPA has higher scope thresholds than the CCPA and does not have a revenue threshold, meaning the law will only apply to companies with significant footprints in the state.

Exemptions

Like the CCPA, the CDPA exempts from its provisions entities that are subject to the Gramm-Leach-Bliley Act (i.e. financial institutions) or the Health Insurance Portability and Accountability Act (i.e. health institutions), as well as government bodies, non-profit organizations, and institutions of higher education.

The CDPA also excludes from its scope personal data that is subject to other laws, including the Fair Credit Reporting Act and the Family Educational Rights and Privacy Act.

Additionally, the law defines "consumer" to exclude individuals acting in a commercial or employment context, avoiding tricky issues relating to human resources information that have been a point of contention among legislators.

Finally, the law provides for a number of limitations from its obligations, including complying with other laws, cooperating with law enforcement, exercising or defending legal claims, performing a contract, and engaging in research in the public interest.

Consumer Rights

Consumers have many rights under the law, including:

- the right to know whether their data is processed;
- the right to access their data
- the right to correct inaccuracies in their data;
- the right to deletion of their personal data;
- the right to receive a copy of their data in a portable format; and
- the right to opt-out of certain processing purposes.

Notably, the CDPA's opt-out provision is more expansive than that of the CCPA. The law allows consumers to opt out of data processing for:

- targeted advertising;
- sale; or
- profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Should a consumer wish to enforce their rights, the controller of the consumer's data must respond to the request within 45 days of receiving the request, with one possible 45-day extension if "reasonably necessary," based on the complexity and number of the consumer's requests.

If the company decides not to fulfil a consumer's request, they must tell the consumer "without undue delay" and at most 45 days after receiving the request, along with a justification for rejecting the request.

Controller Requirements

The CDPA imposes a number of obligations on covered entities, similar to those imposed by the CCPA and GDPR. These obligations include:

- **minimization**—only collecting consumer data that is "adequate, relevant, and reasonably necessary" to the purposes disclosed to the consumer;
- **security**—implementing an adequate cybersecurity system to protect consumer data;
- **sensitive data protections**—controllers must obtain consent before processing sensitive data such as race, health data, biometric data, or children's data;

- **data protection assessments**—controllers must conduct a data protection assessment of high-risk processing, including processing for targeted advertising, sale, profiling, and processing of sensitive data; and
- **contractual protections for processors**—controllers must put in place contracts with processors that impose certain obligations on processors such as duties of confidentiality and cooperation.

The GDPR's influence on the CDPA is clear in these obligations, particularly with regards to consent requirements—defined as a "clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement"—and the requirement to conduct data protection assessments for high-risk processing.

Privacy Notices

The CDPA requires controllers to provide consumers with a "reasonably accessible, clear, and meaningful privacy notice" before data collection, which includes information on:

- categories of personal data that are processed;
- the purpose for processing;
- what categories of personal data are shared with third parties (if any);
- what categories of third parties (if any) to which personal data is shared; and
- how consumers can exercise their rights; including opting out of sales or targeted advertising.

The privacy notice must also include a "secure and reliable" method for consumers to submit their request to enforce their rights under the law.

Penalties

The Attorney General has authority to enforce the CDPA, including seeking injunctive relief and civil penalties of up to USD 7,500 per violation. However, the law provides for a 30-day cure period following initial notice by the Attorney General of potential violations.

The law explicitly excludes a private right of action.

CONCLUSION

2021 is quickly shaping up to be a momentous year for privacy legislation in the US. Virginia is the first state to pass a comprehensive privacy law this year, but it is unlikely to be the last. Washington is attempting for the third time to pass its own bill, and other states like New York, Oklahoma, and Utah are considering similar measures. Meanwhile, commentators expect that federal legislation may be on the horizon after momentum stalled last year due to the COVID-19 pandemic. Companies should keep a close eye on privacy developments around the country as they look to augment their privacy policies to comply with the CDPA.

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

Christine Chen
Associate

T +1 202 912 5081
E christine.chen
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.