What Constitutes Personal Data Under VCDPA?

The VCDPA is concerned with information that is linked, or can be reasonably linked, to an identifiable natural person, but does not include “de-identified data or publicly available information.” The definition of “de-identified data” is broad and includes any information that cannot reasonably be linked to an identifiable natural person or devices linked to that person.

The definition of “publicly available information” is also broad and includes “information that is lawfully made available through federal, state, or local records or . . . made available to the general public through widely distributed media, by the consumer[.]” Availability of information through widely distributed media also includes information disclosed by the consumer to a person and made public by that person, “unless the consumer has restricted the information for a specific audience.” Thus, unless set to private, information on social media accounts and posts may fall outside of the scope of the VCDPA.

The VCDPA exempts some very specific information and data that businesses may possess, including, among others, protected health information under HIPAA, information de-identified pursuant to HIPAA, and information used only for public health as authorized by HIPAA, as well as information collected and used or activities regulated and authorized under the federal Fair Credit Reporting Act.

The VCDPA also created another class of protected personal data called “sensitive data.” Sensitive data is personal 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.

Signed into law earlier this year, the Virginia Consumer Data Protection Act (VCDPA) is a comprehensive privacy law that will affect many businesses either based in Virginia or doing business with or marketing to consumers in the Commonwealth. As the name suggests, the VCDPA is designed to provide protections to consumer data, allowing consumers to access, modify, or delete their personal information, and choose to opt out of the sale and processing of that information for targeted advertising and profiling purposes. Entities that will be doing business in Virginia after January 2023 when the law goes into effect need to assess now whether the provisions of the VCDPA apply, and if so, take the steps necessary to become compliant with the new law.

Does Your Business Need to Comply?

The VCDPA applies to all entities that a) conduct business in the Commonwealth or b) which produce products or services targeted to residents of the Commonwealth and 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% of gross revenue from the sale of personal data.

The VCDPA does not apply, however, to state and local governments or agencies of the Commonwealth, financial institutions or data subject to the Graham Bliley Act, health care entities or business associates covered by the Health Insurance Portability and Accountability Act (HIPAA) or the Health Information Technology for Economic and Clinical Health Act (HITECH), nonprofit organizations, or colleges and universities.
Notably, the VCDPA does not permit the processing of sensitive data concerning a consumer without clear affirmative consent from that consumer.

**Consumer Rights**

It is important to point out that the VCDPA only considers individual residents of Virginia acting in their personal or household capacity as a “consumer.” Thus, personal data and information collected when an individual is acting in a commercial capacity, such as an agent or employee of a business or other entity, is not subject to the protections of the VCDPA. When personal data is subject to the protections of the VCDPA, a consumer has the right to:

- confirm whether a business possesses the consumer’s personal data and access such data;
- correct inaccuracies;
- delete it (whether provided by or collected about the consumer);
- obtain copies of it; and
- “opt out of the processing of personal data for purposes of (i) targeted advertising, (ii) the sales of personal data, or (iii) profiling in furtherance of decisions that produce legal or similar effects concerning the consumer.”

Because personal data may be spread across multiple places, controllers should both clearly disclose to consumers what data will be collected and implement processes that allow for them to easily and confidently locate and delete that data.

The VCDPA also provides consumers the right to obtain the data in a portable and readily useable format to allow the consumer to transmit it to another business. **The VCDPA explicitly prohibits any attempt to restrict any of its consumer rights by contract.**

With respect to consumers opting out of certain processes, while the sale of personal data is straightforward, the distinction between targeted advertising and profiling is less clear. The “sale of personal data” under the VCDPA is limited to the “exchange of personal data for monetary consideration by the controller to a third party.” Certain exchanges of personal data, however, are excluded from this definition, including:

- disclosure to a processor that processes personal data on behalf of the controller;
- disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
- disclosure or transfer of personal data to an affiliate of the controller;
- disclosure of information that the consumer intentionally made available to the general public and did not restrict to a specific audience; or
- disclosure or transfer to a third party as an asset as part of a merger, acquisition, or bankruptcy.

**Controllers should both clearly disclose to consumers what data will be collected and implement processes that allow for them to easily and confidently locate and delete that data.**

Like targeted advertising, profiling is commonly associated with behavioral advertising—a very common form of advertising used on websites and smartphone apps (for example, being bombarded with sunscreen ads after searching online for a beach vacation). While profiling necessarily involves some automated processing, the exact scope of the right to opt out in the processing of data for purposes of “profiling in furtherance of decisions that produce legal or similar effects concerning the consumer” is unknown.

On the one hand, the VCDPA broadly defines profiling as “any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to a [consumer]’s economic situation, health, personal preferences, interests, reliability, behavior, location or movements.”

On the other hand, the profiling opt out applies only to “decisions that produce legal or similar effects.” In other words, the VCDPA applies to some but not all profiling processes. It appears that the profiling process must have the potential to significantly influence the circumstances, behavior, or choices of consumers, otherwise it may just be targeted advertising.

The VCDPA also protects consumers from discrimination by a controller for exercising any of the rights it grants, but explicitly exempts loyalty programs from this antidiscrimination policy.

**Controller Responsibilities**

Controllers are required to disclose the collection of personal data to consumers and limit it what is reasonably necessary and to establish, implement, and maintain security practices to protect it. Controllers are required to give consumers notice of the categories of personal data to be processed and shared with third parties (and if any what and to whom it is being shared), the purpose for the data processing, and how consumers may exercise
their rights under the VCDPA, including the right to appeal.

Controllers may not discriminate in processing personal data and, unless the controller obtains the consumer’s consent, cannot process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data was collected.

Controllers may not discriminate in processing personal data and, unless the controller obtains the consumer’s consent, cannot process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data was collected.

Consumer requests, however, are not unlimited. Controllers only have to respond to the requests of authenticated consumers and may charge for excessive or repetitive requests. Controllers are also required to establish a process for consumers to appeal the denial of a request and advise consumers of this right of appeal.

Controllers also must conduct and document data protection assessments regarding data processing activities involving personal data.

These data assessments are not cursory and must 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. The 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, shall be factored into this assessment by the controller.

Upon request, controllers must make the data assessment available to the Attorney General for a confidential review, which is excluded from the Virginia Freedom of Information Act and does not constitute a waiver of attorney-client privilege or work product immunity.

For questions or assistance, please contact:

Jonathan M. Joseph, Esq.
jjoseph@cblaw.com | 804.697.4125

Robert D. Michaux, Esq.
rmichaux@cblaw.com | 804.697.4119

©Christian & Barton, LLP 2021 | All Rights Reserved | 901 East Cary Street, Suite 1800 | Richmond, Virginia 23219