The Labyrinth Expands: Virginia Passes New Privacy Law with Additional Obligations for Businesses

As businesses continue to weave their way through the labyrinth of privacy laws, from the EU's General Data Protection Regulation to the California Consumer Privacy Act to the numerous other sectoral and international privacy laws, the path just grew longer and more complex.

On March 2, 2021, the Governor of Virginia signed the Virginia Consumer Data Protection Act ("CDPA") into law. Following California's lead, Virginia has become the second state to enact a broad consumer privacy law. To comply, even businesses that have worked toward fulfilling the California Consumer Privacy Act's ("CCPA") requirements will likely need to draft new portions of their privacy policies, conduct or document data protection assessments, revise their process and interface for consumer requests, and amend their vendor agreements and/or data processing agreements. The continual enactment of new privacy laws may leave businesses wishing Ariadne's thread would appear to lead them through the tangle.

The Basics: The CDPA is effective January 1, 2023, and can lead to up to a $7500 penalty for each violation. It will be enforced by the Virginia Attorney General and does not include a private right of action. The CDPA applies to those who conduct business in Virginia or produce products or services targeted to Virginia residents and (1) control or process data of at least 100,000 consumers annually or (2) make over 50% of their gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers. The definition of "consumer" includes only those acting in an individual or household context, not those acting in a commercial or employment context. Numerous sectoral exemptions are included for certain financial and health-related entities, non-profits, institutions of higher learning, and others. The Virginia Legislature incorporated exemptions for certain types of data as well.

Additional Personal Data Rights Request Types: While CCPA-compliant businesses will already have procedures for processing consumer requests to access, delete, and opt out of the sale of personal information, the passage of the CDPA means they will also

Related Capabilities

- Privacy & Social Media
- California Consumer Privacy Act (CCPA)

have to implement procedures to enable consumers to correct their personal data and opt of the processing of their data for purposes of targeted advertising or "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." Businesses will need to be prepared to answer consumer requests up to twice annually.

Appeals Process: Businesses must also implement and disclose an appeals procedure to address consumer request denials. Within 60 days of receiving an appeal, businesses must notify consumers of the actions taken in response to the appeal and provide a written explanation of the reasoning therefor. In the event of a denial, businesses must provide consumers with a method by which to contact the Virginia Attorney General for the purposes of submitting a complaint.

Sensitive Data: Under the CDPA, a business may not process sensitive data without consumer consent. For the purposes of the CDPA, "sensitive data" means:

A category of personal data that includes:

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

Data Protection Assessments: Businesses must perform and document data protection assessments for each of the following personal data processing activities:

1. The processing of personal data for targeted advertising;
2. The sale of personal data;
3. The processing of personal data for purposes of profiling, where such 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 injury to consumers;
4. The processing of sensitive data; and
5. Any processing activities involving personal data that present a heightened risk of harm to consumers.

Such assessments "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," and may be requested by the Virginia Attorney General in connection with an investigation. Conducting such assessments under attorney-client privilege will be important in this regard.

Vendor Agreements: Processors must enter written contracts with controllers that include

certain requirements including assisting controllers in meeting the obligations of the CDPA, such as responding to consumer rights requests, providing breach notifications, conducting data protection assessments, and entering written contracts with subcontractors that meet the requirements of the CDPA.

The differences between the CDPA and California's CCPA highlighted above are not meant to represent an exhaustive accounting of the ways in which the CDPA diverges from the CCPA and do not take into account the many nuances and exemptions contained within the new law. Rather, these differences are meant to show that, even if your business has successfully tackled the CCPA, its privacy compliance journey through the labyrinth is not yet over (especially with the California Privacy Rights Act also slated to come into effect and the temporary exemptions of certain employee and B2B information under the CCPA set to expire January 1, 2023).

Please contact your Dorsey privacy counsel for assistance in navigating the CDPA requirements.