Following California’s lead, two states recently enacted new privacy laws designed to protect consumers’ rights over their personal data. The Colorado Privacy Act and the Virginia Consumer Data Protection Act mimic California privacy laws and the EU General Data Protection Regulation (GDPR) by imposing stringent requirements on companies that collect or process personal data of state residents. Failure to comply may subject companies to enforcement actions and stiff fines and penalties by regulators.

**Virginia Consumer Data Protection Act**

On March 2, 2021, Virginia’s legislature passed the Consumer Data Protection Act
(CDPA, the Act), which goes into effect on January 1, 2023.

**Organizations Subject to the CDPA**

The Act generally applies to entities that conduct business in the state of Virginia or that produce products or services targeted to residents of the state and meet one or both of the following criteria: (1) control or process personal data of 100,000 Virginia consumers annually, (2) control or process personal data of at least 25,000 consumers (statute silent as to whether this is an annual requirement) and derive more than 50 percent of gross revenue from the sale of personal data. The processing of personal data includes the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

Notably, certain organizations are exempt from compliance with the CDPA, including government agencies, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA), entities subject to the Health Insurance Portability and Accountability Act (HIPAA), nonprofit organizations and institutions of higher education.

**Broad Definition of Personal Data**

The CDPA broadly defines personal data to include any information that is linked to an identifiable individual, but does not include de-identified or publicly available information. The Act distinguishes personal sensitive data, which includes specific categories of data such as race, ethnicity, religion, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric data, children’s data and geolocation data.

**Consumers’ Data Protection Rights**

The new Virginia privacy law recognizes certain data protection rights over consumers’ personal information, including the right to access their data, correct inaccuracies in their data, request deletion of their data, receive a copy of their data, and opt out of the processing of their personal data for purposes of targeted advertising, the sale of their data or profiling.

If a consumer exercises any of these rights under the CDPA, a company must respond within 45 days - subject to a one-time 45-day extension. If the company declines to take action in response to the consumer’s request, the company must notify the consumer within 45 days of receipt of the request. Any information provided in response to a consumer’s request shall be provided by the company free of charge, up to twice annually per consumer. The company must establish a procedure for a consumer to appeal the company’s refusal to take action on the consumer’s request. The company is required to provide the consumer with written notice of the decision on appeal within 60 days of receipt of an appeal.

**Responsibilities of Data Controllers**

The CDPA imposes several requirements on companies/data controllers, including limiting the collection of personal data, safeguarding personal data by implementing
reasonable data security practices and obtaining a consumer’s consent prior to processing any sensitive data.

Moreover, data controllers should have a Privacy Notice that clearly explains the categories of personal data collected and processed; the purpose for processing personal data; how consumers can exercise their rights over their personal data; any categories of personal data shared with third parties; the categories of third parties with which personal data is shared; and consumers’ right to opt out of the processing of their personal data.

Importantly, all data controllers are required to conduct and document a data protection assessment (DPA). The DPA should identify and weigh the benefits and risks of processing consumers’ personal data and the safeguards that can reduce such risks. The Virginia Attorney General (VA AG) may require a controller to produce a copy of its DPA upon request.

Furthermore, data controllers must enter into a binding written contract with any third parties that process personal data (data processors) at the direction of the controller. This contract should address the following issues: instructions for processing personal data; nature and purpose of processing; type of data subject to processing; duration of processing; duty of confidentiality with respect to the data; and deletion or return of data to the data controller. In addition, the contract should include a provision that enables the data controller or a third party to conduct an assessment of the data processor’s policies and procedures for compliance with the protection of personal data.

**Regulatory Enforcement**

The VA AG has the exclusive authority to enforce the CDPA. Prior to initiating an enforcement action, the VA AG is required to provide the company/data controller with written notice identifying violations of the Act. If the company cures the violations within 30 days and provides the VA AG with express notice of the same, then no action will be taken against the company. The law permits the VA AG to impose statutory civil penalties of up to $7,500 for each violation of the Act. Moreover, the VA AG also may seek recovery of its attorneys’ fees and costs incurred in investigating and enforcing the resolution of violations of the Act.

**Colorado Privacy Act**

On July 7, 2021, Colorado passed the Colorado Privacy Act (CPA), which takes effect on July 1, 2023. In many respects, the CPA mirrors Virginia’s new privacy law.

**Organizations Subject to the Law**

The CPA applies to companies/data controllers that:

- Conduct business in the state of Colorado or
- Produce or deliver commercial products or services that are targeted to residents of Colorado and
Satisfy one or both of the following criteria:

- Control or process personal data of 100,000 or more Colorado consumers annually
- Derive revenue from the sale of personal data and process or control personal data of 25,000 or more Colorado consumers (statute silent as to whether this is an annual requirement).

Notably, the CPA does not apply to personal data that is protected under certain other laws, including GLBA, HIPAA, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act (FERPA), customer data maintained by a public utility, employment records or data maintained by an institution of higher education.

**Broad Definition of Personal Data**

The CPA broadly defines personal data as information that can be linked to an identifiable individual, but does not include de-identified or publicly available information. The law also distinguishes personal sensitive data that may include race, ethnicity, religion, mental or physical health condition or diagnosis, sexual orientation or citizenship.

**Consumers’ Data Protection Rights**

The law sets forth consumers’ data protection rights, including the right to access their personal data; the right to correct inaccuracies in their data; the right to request deletion of their data; the right to obtain a copy of their data; and the right to opt out of the processing of their personal data for the purposes of targeted advertising, the sale of their data or profiling.

A company/data controller must respond to a consumer’s request within 45 days – subject to a single 45-day extension as reasonably required. The company must notify the consumer within 45 days if the company declines to take action in response to a consumer’s request. Information provided in response to a consumer request shall be provided by the company free of charge, once annually per consumer. The company must establish a procedure for a consumer to appeal the company’s refusal to take action on a consumer’s request. The company shall provide the consumer a written decision on an appeal within 45 days of receipt of the appeal. The company may extend the appeal response deadline by 60 additional days where reasonably necessary.

**Responsibilities of Data Controllers**

The CPA imposes a number of stringent requirements on companies, including limiting the collection of personal data to what is reasonably necessary; taking reasonable measures to secure personal data from unauthorized acquisition during both storage and use; and obtaining a consumer’s consent prior to processing any sensitive data.
The data controller should have a clear and conspicuous Privacy Notice that sets forth the categories of personal data processed by the company, the purpose for processing personal data and the means by which consumers can withdraw their consent to processing of their data. The Privacy Notice should identify the categories of personal data collected or processed, categories of personal data shared with third parties and the categories of third parties with which personal data is shared. The Privacy Notice also must disclose whether the company sells personal data or processes personal data for targeted advertising, and the means by which consumers can opt out of the sale or processing of their data.

A data controller shall not process any personal data that represents a heightened risk of harm to a consumer without conducting a data protection assessment (DPA). The DPA must identify and weigh the benefits from the processing of personal data that may flow to the controller, the consumer and the public against the potential risks to the rights of the consumer. These risks may be mitigated by safeguards adopted by the company. The company may be required to produce its DPA to the Colorado Attorney General (CO AG) upon request.

A company/data controller must enter into a binding contract with any third parties (data processors) that process personal data at the direction of the data controller. This contract should address the following issues: data processing procedures, instructions for processing personal data, nature and purpose of processing, type of data subject to processing, duration of processing, and deletion or return of data by the data processor. The contract also should include a provision that allows the controller to perform audits and inspections of the processor at least once annually and at the processor’s expense. The audit should examine the processor’s policies and procedures regarding the protection of personal data. If an audit is performed by a third party, the processor shall provide a copy of the audit report to the controller upon request.

**Regulatory Enforcement**

The CO AG has the exclusive authority to enforce the DPA by bringing an enforcement action on behalf of Colorado consumers. A violation of the DPA is considered to be a deceptive trade practice. Prior to initiating an enforcement action, the CO AG must issue a notice of violation to the company and provide an opportunity to cure the violation. If the company fails to cure the violation within 60 days of receipt of notice of the violation, the CO AG may commence an enforcement action. Civil penalties may be imposed for violations of the Act.

**Conclusion**

Companies that collect or process consumer data are well advised to heed these new privacy laws imposed by Virginia and Colorado, since more states are sure to adopt similar laws. Failure to adhere to these new stringent legal requirements summarized in the table below may subject companies to regulatory enforcement actions, in addition to fines and penalties.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Virginia</th>
<th>Colorado</th>
</tr>
</thead>
</table>

Consumer Data Protection Rights

- Right to access personal data
- Right to correct personal data
- Right to delete personal data
- Right to receive a copy of personal data
- Right to opt out of processing personal data

Duty to Respond to Consumer Requests

- Within 45 days (subject to one-time extension)
- Notice of refusal to take action
- Provide information free of charge
- Appeal process

Privacy Notice

- Categories of personal data collected or processed
- Purpose for processing data
- How consumers can exercise their rights
<table>
<thead>
<tr>
<th>Category</th>
<th>Include</th>
<th>Exclude</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of personal data shared with third parties</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Categories of third parties with which personal data is shared</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>How consumers can opt out of the sale or processing of their personal data</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Data Protection Assessment (DPA)**

Documented DPA weighing the benefits and risks of processing consumers’ personal data, and the X safeguards that can reduce such risks

**Binding Contract Between Data Controller and Third-Party Data Processor**

Instructions for processing personal data                             | X       | X       |
| Nature and purpose of the processing                                | X       | X       |
| Type of data subject to processing                                  | X       | X       |
| Duration of processing                                              | X       | X       |
| Duty of confidentiality                                             | X       | X       |
| Deletion or return of data                                          | X       | X       |
| Audits of data processor’s policies and procedures to safeguard data | X       | X       |
and comply with privacy laws

**Enforcement**

Enforcement by Attorney General  X  X

Fines and penalties  X  X

© 2022 Wilson Elser

National Law Review, Volume XI, Number 215