Published on *The National Law Review* https://natlawreview.com

2023 State Privacy Laws and Regulations Bring Extensive Data Protection Assessment Requirements

Article By:

Alan L. Friel

On January 1st of this year, the Virginia Consumer Data Protection Act ("VCDPA") and amendments to the California Consumer Privacy Act ("CCPA") went into effect. Later this year, the Colorado Privacy Act ("CPA"), Connecticut's Public Act No. 22-15 (known as the "Connecticut Privacy Act" or "CTPA"), and the Utah Consumer Privacy Act ("UCPA") will go into effect as well. Aside from the UCPA, these laws will obligate covered entities to document and assess certain processing activities in formal data protection assessments, which will be available to regulators. The purpose is to require companies to look critically at high-risk data processing activities and avoid unjustifiable risks and negative impacts on data subjects. Assessments can also serve the purpose of maintaining current data inventories and retention schedules and ensuring that processing is not inconsistent with the notified purposes at the time of collection.

The requirements for the content of the data protection assessments are extensive, especially under the CPA. We discuss them in detail in our Data Protection Assessment Tool Kit, which includes data protection assessment templates and is available to clients for a fixed fee.

The following is a basic summary of requirements by the new state privacy laws:

- ***VCDPA and CTPA*:** Virginia's and Connecticut's requirements for data protection assessments are almost identical. Controllers subject to the VCDPA and CTPA must conduct and document a data protection assessment when processing sensitive data, processing personal data for targeted advertising, selling personal data, processing personal data for profiling when it presents a reasonably foreseeable risk of harm to consumers, and other processing activities that present a heightened risk of harm. In each assessment, controllers must analyze the risks and benefits of the processing activity to consumers and other interested parties, in addition to safeguards that can be applied to minimize the risks. Controllers should factor in the use of deidentified data, consumers' reasonable expectations, and the context of the processing activity in such analysis. There are no explicit storage and update requirements, but controllers should update assessments as needed to address risks throughout the lifecycle of the processing activity and should store assessments for a reasonable period (Colorado requires retention for 3 years so that seems a good standard to use) after the end of the processing activity. The respective state attorney general can request to evaluate assessments, and controllers should be ready to disclose them. These

requirements are already operative under the VCDPA, and will become operative on July 1, 2023 under the CTPA.

- ***CPA*:** Colorado's requirements under the CPA and its final rules ("CPA Regs"), which were recently finalized by the Colorado Attorney General, are the most extensive. Like the VCDPA and CTPA, controllers subject to the CPA must conduct data protection assessments when processing sensitive data, selling personal data, processing personal data for targeted advertising, and processing personal data for profiling when it presents a reasonably foreseeable risk of harm to consumers. Assessments must conduct a risk-benefit analysis, including a discussion of safeguards and measures taken to offset the risks. Unlike the VCDPA and CTPA's broad requirements, the CPA Regs provide a list of 12 explicit inquiries that must be discussed, along with an additional 12 that are required if the processing activity at issue is profiling. While the other states do not require this level of detail, the inquiries are reflective of the general considerations mandated by the other states. To conduct data protection assessments, controllers must include the input of all relevant internal and external parties. Once the requirement to conduct a data protection assessment is triggered, a controller must review and update the assessment as often as appropriate to address risks considering the type, amount, and sensitivity of personal data processed. If the processing activity is profiling, the assessment must be reviewed and updated at least annually. Assessments must be stored for at least three years after the processing activity has concluded, and controllers should be prepared to disclose assessments to the Colorado Attorney General upon request. These requirements become operative on July 1, 2023.

- ***CCPA*:** The details of data protection assessments have not yet been addressed under the CCPA as revised by the California Privacy Rights Act ("CPRA"), which calls for details to be determined in rulemaking ("CPRA Regs"). However, the California Privacy Protection Agency ("CPPA") has discussed its plans for rulemaking pertaining to data protection assessments and is soliciting preliminary public input on this topic. Thus far, the CPPA is considering basing its data protection assessment rules on the European Data Protection Board's ("EDPB") guidelines and incorporating CPA requirements. Accordingly, controllers subject to the CCPA should be prepared to abide by CPA requirements, discussed above. In addition, EDPB guidelines can be looked to now to guide the development of a multi-state assessment program. The EDPB guidelines provide that assessments are required prior to processing that is likely to result in a high risk of harm to consumers, and activities that include automated processing and profiling, processing sensitive data, the monitoring of a publicly accessible area on a large scale, the processing of data on a large scale, the matching or combining of data sets that would exceed the reasonable expectations of consumers, the use of data concerning vulnerable consumers, the use of innovative or new technology, and processing that prevents consumers from exercising a right or using a service. If a high-risk activity is conducted, but a controller decides not to conduct a data protection assessment, it must justify and document the reasons for this decision. At a minimum, under the EDPB guidance, data protection assessments should include a description of the processing activity and involved personal data, context of processing, purposes of processing, a risk-benefit analysis and measures to address those risks, and the involvement of all interested parties. There are other suggested additions and mandatory factors to consider when completing an assessment. Please see our guidance for a more detailed explanation. Controllers should review and update each assessment periodically, especially if there was a change of the risk involved, and should be prepared to disclose assessments to the California Attorney General upon request.

- ***UCPA*:** Utah's law does not address data protection assessments, and there will likely be no regulations forthcoming as no statutory rulemaking authority was granted.

For all of the above laws, each applicable processing activity must have its own data protection assessment, but a single assessment can cover comparable processing activities. Similarly, each law provides that if a controller conducts a data protection assessment to comply with one state law, that assessment will satisfy the requirements established by the other state laws as long as it is reasonably similar in scope and effect to those state law requirements. Because of this, it may be in the best interest of controllers to comply with the requirements of all of the above state laws in a wholesale manner, applying all state requirements to all assessments. Our templates and guidance materials take this approach.

Businesses should note that under the CTPA and CPA, Data Protection Assessments are required for specified processing activities created or generated after July 1, 2023. There is some ambiguity whether the "created or generated" language includes activities that began prior to this date and are ongoing. However, the word "generated" can be interpreted to include ongoing activities, and we recommend conducting assessments for such ongoing activities under all the state laws to remain compliant.

Sasha Kiosse also contributed to this article.

National Law Review, Volume XIII, Number 79