Articles + Publications | May 16, 2022

Emerging Requirements for Data Protection Impact Assessments

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Niya T. McCray

Under the emerging regime of privacy laws in the U.S., businesses must prepare to assess the protection of certain information in view of proposed data processing activities, beginning with the new laws to be effective in 2023 in California, Colorado and Virginia. These requirements are similar in many ways to the existing requirements for data privacy impact assessments under the European Union's General Data Protection Regulation (the "GDPR") and the United Kingdom's General Data Protection Regulation (the "UK GDPR"). Although the terms differ among jurisdictions, the basic concepts are substantially similar, so we refer to the relevant information as personal information, and the required assessments as data protection impact assessments ("DPIAs"). The California Privacy Rights Act (the "CPRA") and Virginia Consumer Data Protection Act (the "VCDPA"), which become effective January 1, 2023, and the Colorado Privacy Act (the "CPA") to be effective July 1, 2023, all require covered entities to perform DPIAs, but they differ from each other and from the GDPR and the UK GDPR in key terminology and certain requirements.

California[1]

Although the California Consumer Privacy Act of 2018 (the "CCPA") did not include a requirement to conduct a DPIA, this requirement will be added by the CPRA effective January 1, 2023. The CPRA requires the California Attorney General to promulgate regulations requiring businesses whose processing of personal information presents significant risk to privacy and security to perform an annual cybersecurity audit, and to submit to the California Privacy Protection Agency (the "CPPA") on a regular basis a risk assessment with respect to the processing of personal information. Subject to the expected regulations, a DPIA required under the CPRA must:

1. indicate whether the processing involves sensitive personal information, and
2. identify and weigh the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with such processing, with the goal of restricting or prohibiting such processing if the risks to the privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.

Colorado[2]

Effective July 1, 2023, the CPA prohibits "processing that presents a heightened risk of harm to a consumer" unless the controller first conducts and documents a DPIA. Under the CPA, "processing that presents a heightened risk of harm to a consumer" includes:

©2026 Troutman Pepper Locke

- Targeted advertising;
- Sales of personal data;
- Processing personal data for profiling which creates certain risks for consumers, including:
  - unfair or deceptive treatment;
  - unlawful disparate treatment;
  - financial injury;
  - physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person;
  - and other risks; and
- Processing sensitive data.

As drafted, the CPA list above is not exclusive, and other processing activities could be determined to present high risk and therefore require DPIAs. The CPA requires that all DPIAs identify and weigh the benefits that flow from the processing of data to the controller, consumer, and other stakeholders against the potential risks to the right of the consumer from processing. In performing the cost-benefit analysis, controllers should also consider "the use of de-identified data and the reasonable expectations of consumers."

The CPA also includes a broad, mandatory disclosure where the state Attorney General seeks to "evaluate the data protection assessment for compliance with the duties contained in section 6-1-1308 and with other laws, including this article 1 [i.e., the entire CPA]." Nevertheless, the disclosure of a DPIA to the Attorney General does not constitute a waiver of confidentiality or any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment.

Virginia[3]

Like CPA, the VDCPA, effective January 1, 2023, requires data controllers to conduct DPIAs for any activities that present a "heightened risk of harm" to consumers. DPIAs are required for the following processing activities:

- Targeted advertising;
- Sales of personal data;
- Processing personal data for purposes of profiling which creates certain risks for consumers, including:
  - unfair or deceptive treatment;
  - unlawful disparate treatment;
  - financial, physical, or reputational injury;
  - 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;
  - and other risks;
- Processing sensitive data; and
- Any processing activities involving personal data that present a heightened risk of harm to consumers.

Unlike the CPA, under the VCDPA provides that the risk of reputational injury warrants a DPIA in the context of profiling.

Although the VCDPA fails to define a "heightened risk of harm," it is clear that a DPIA 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." In conducting and documenting the DPIA, controllers must consider "[t]he 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."

VCDPA § 59.1-580 includes mandatory disclosure where the state Attorney General, in connection with an investigation, requests any DPIAs relevant to the investigation. While the Attorney General disclosure is mandatory, the disclosure of a DPIA does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment. Further, the disclosures will be deemed confidential and exempted from state public inspection and copying law.

* * * * *

Although the state DPIA requirements in California, Colorado and Virginia bear strong similarities, there are differences that require careful attention to the applicable requirements. In addition, the California DPIA requirement will be subject to forthcoming regulations that may expand or narrow the scope of the requirement, and otherwise shape the obligations of businesses. Even in the absence of guidance under any of these statutes, and the expected California regulations, businesses must begin now to prepare for these coming requirements, by taking an inventory and assessing all processing of the personal information. All processing should be assessed for the benefits to the business and its stakeholders, and to consumers, and for the related risks to consumers. Businesses that have conducted DPIAs under the GDPR or the UK GDPR requirements will have a head start, because of the similarities among these requirements, but all business subject to the CPRA, the CPA and/or the VCDPA will have significant work to do to achieve compliance.

***

?[1] CPRA §§ 1798.185(a)(15)(A), (B).

?[2] CPA § 6-1-1309

?[3] VCDPA § 59.1-576/sup>

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber