BCLP. Client Intelligent

Insights

COMPARING THE DATA PROTECTION ASSESSMENT REQUIREMENTS ACROSS THE NEXT GENERATION OF U.S. STATE PRIVACY LAWS

NEW U.S. STATE PRIVACY LAWS MANDATE DPIAS IN CERTAIN CIRCUMSTANCES

Nov 30, 2021

WHAT IS A DATA PROTECTION IMPACT ASSESSMENT (DPIA)?

A data protection impact assessment or data protection assessment (DPIA) is a form of risk assessment that is designed to help organizations identify, analyze and minimize the privacy risks associated with their data collection, use, retention, and disclosure practices.

The DPIA is a familiar concept for those versed in the General Data Protection Regulation (GDPR), which mandates DPIAs for any "high risk" processing as a part of the "privacy by design" principle.

Historically, consumer privacy laws in the United States did not mandate the performance of DPIAs, but that is about to change.

NEXT GENERATION PRIVACY LAWS

The next generation of U.S. privacy laws includes:

- The Virginia Consumer Data Protection Act (VCDPA), effective January 1, 2023;
- The Colorado Privacy Act (CPA), effective July 1, 2023; and
- The California Privacy Rights Act (CPRA), effective January 1, 2023,

All require covered entities to perform DPIAs in certain circumstances.

The chart below explains:

- When a business must conduct a DPIA under each of the new laws,
- The required content, and
- Whether the DPIA will be subject to compulsory disclosure.

Privacy law	DPIA triggers	Required content	Compulsory disclosure?
Virginia Consumer Data Protection Act (VDCPA), in force Jan 1, 2023	**"Heightened risk of harm"** VDCPA requires controllers[1] to prepare DPIAs for any activities that present a "heightened risk of harm" to consumers. **Definition** "Heightened risk of harm" is not defined, however, DPIAs are specifically mandated for: ▪ Targeted advertising; ▪ Sales of personal data; ▪ Processing personal data for profiling which creates certain risks for consumers (including unfair or deceptive treat; unlawful disparate treatment; financial, physical, or reputational injury; and other risks); and	**Benefits v risks** The 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."[3] **Conducting and documenting the DPIA** 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."[4]	**Government Investigations** Upon request by the state Attorney General, in connection with an investigation, controllers must disclose any DPIAs relevant to the investigation.[5] **Privilege waiver?** 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.[6] **Confidentiality** The disclosures will be deemed confidential and exempted from state public inspection and copying law (i.e., State FOIA laws).[7]

Privacy law	DPIA triggers	Required content	Compulsory disclosure?
	▪ Processing sensitive data.[2]		
Colorado Privacy Act (CPA), in force Jul 1, 2023	**Closely Mirrors VDCPA** Like the VDCPA, the CPA requires controllers to conduct DPIAs for any activities that present a heightened risk of harm to consumers, and specifically mandates DPIAs in the same contexts as the VDCPA.[8] Unlike the VDCPA, the risk of reputational injury would not warrant a DPIA in the context of profiling.	**Required Content Mirrors VDCPA** The content requirements for DPIAs under the CPA mirror those of the VDCPA.	**Mirrors VDCPA** The disclosure requirements for DPIAs under the CPA mirror those of the VDCPA.
California Privacy Regulations Act (CPRA), in force Jan 1, 2023	**"Significant Risk"** Within the rulemaking provisions of the CPRA, the Attorney General is charged with the issuance of regulations requiring risk assessments for processing activities that present "significant risk" to consumers' privacy or security.[9] Therefore, this requirement may be added by the July 1, 2022 deadline for adopting final regulations.	**Required Content Mirrors the GDPR** A "risk assessment" required under the CPRA must: ▪ indicate whether the processing involves sensitive personal information, and ▪ identify and weigh the benefits resulting from the processing to the business, the consumer, other stakeholders, and	**Submission to CPPA** Businesses will be required to submit their "risk assessments" to the California Privacy Protection Agency on a regular basis.[11] **Further reporting?** Again, we expect that the DPIA reporting requirements will be expanded by the regulations.

Privacy law	Definition DPIA triggers	Required content	Compulsory disclosure?
	"Significant risk" is not defined in the CPRA but may be fleshed out by the regulations.	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.[10]	

Adapting an existing privacy program to meet the new requirements

The good news for organizations seeking to understand how to adapt their privacy programs to these new laws is that the data protection assessment requirements of these laws are similar enough that organizations will likely not need to develop separate DPIA policies and procedures to address each law.

Updates and Alerts

- Stay tuned, as a future alert will address the steps organizations can take to successfully conduct and document a DPIA.
- Be sure to follow our alerts as we continue to examine other key aspects of the next generation of U.S. state privacy laws and steps that companies can undertake to begin addressing them.
- Our prior alerts are available here.

1. Controllers under the VDCPA and CPA are generally defined as the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

2. VDCPA, § 59.1-576(A)(1-5).

3. VDCPA, § 59.1-576(B).

4. VDCPA, § 59.1-576(B).

5. VDCPA, § 59.1-576(C).

6. VDCPA, § 59.1-576(C).

7. VDCPA, § 59.1-576(C).

8. CPA, § 6-1-1309(2)(a)-(c).

9. CPRA, § 1798.185(a)(15)(B).

10. CPRA, § 1798.185(a)(15)(B).

11. CPRA, § 1798.185(a)(15)(B).

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Co-Author, Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Goli Mahdavi

Co-Author, San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448
